Section 1 (U) Mission Statement, The National Security List, Acronyms, and File Classifications

Section 1-01 (U) Mission Statement

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

Section 1-02 (U) The National Security List

A. (U) The National Security List [redacted] generally defines the types of investigative activities which are engaged in with respect to the FBI's National Foreign Intelligence Program. The List is designed to enable the FBI to flexibly respond to a changing world. It is constantly evaluated in the light of U.S. National Security needs [redacted] See: Appendix C-12, infra. b7E

B. (U) [redacted]

C. [redacted]

D. (U) [redacted]

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 1-03 (U) Acronyms

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

(U) **Section 1-04 (S) File Classifications and Alpha Designations for Investigative and Administrative Activities which Uniquely Fall Within the Purview of the FBI's National Foreign Intelligence Program**

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

Section 2 (U) General Investigative and Administrative Activities and Requirements

2-01 (U) General Investigative and Administrative Activities and Requirements

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-02 (U) NATIONAL SECURITY INVESTIGATIONS

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-03 (U) SUMMARY GUIDANCE AND APPLICABILITY OF THREAT ASSESSMENTS:

(S)

b1

(S)

b1

B. (U) Retention of Threat Assessment Information

1. The NSIG authorize, with certain limitations, the retention and dissemination of threat assessment information for broad analytic and intelligence purposes, regardless of whether it furthers investigative objectives in a narrower or more immediate sense. Accordingly, even if information obtained during a Threat Assessment does not warrant opening either a Preliminary Investigation or a Full Investigation, those who possess personally identifying information derived from Threat Assessments may retain it for valid national security purposes. In that regard, the information may eventually serve a variety of valid analytic purposes as pieces of the overall intelligence picture are connected to thwart terrorist activities. In addition, the information may possibly assist FBI personnel in responding to any questions which may subsequently arise as to the nature and extent of the Threat Assessment and its results, whether positive or negative.

2. One cautionary point in this regard must be emphasized. This type of information, i.e., information obtained during a Threat Assessment that has insufficient value to justify further investigative activity (at least at the time it is obtained), is often sensitive personal information concerning U.S. persons and entities. If it is retained for the purposes addressed above, measures should be taken to identify it accurately as Threat Assessment information, to protect it from inadvertent disclosure, and to preclude its use as a basis for any further investigative activity unless and until such action is authorized by the NSIG or other applicable regulations.

2-04 (U) SUMMARY GUIDANCE AND APPLICATION FOR PRELIMINARY INVESTIGATIONS (PI)

(S)

b1

B. (U) Sensitive National Security Matters. A PI initiated by a field office that involves a Sensitive National Security Matter may be approved by a SAC. b7E

1. A *Sensitive National Security Matter as defined in the NSIG is a threat to the national security involving* [redacted] *a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials.*

(S) [redacted] b1

(U) D. (X) All Sensitive National Security Matters not specifically mentioned above may be approved by the SAC, but may not be delegated.

(U) E. (X) PIs not involving Sensitive National Security Matters may be approved by an SAC or as authorized by the SAC, the ASAC or squad supervisor with national security investigative responsibility.

(S) [redacted] b1

(S) [redacted] b1

cooperative witnesses)
Recruitment

(S) [redacted] b1

[redacted] b1 Referral/Consult

5. Undercover Operations (UC): (*Discussed in Section 28*)

a. Group I UC operations involving *Sensitive Circumstances* necessitate the following requirements:

(U) [redacted] b7E

b. Group II UC operations necessitate the following requirements:

(S) [redacted] b1

1. SAC Approval

(S)

b1

6. Undisclosed participation (UDP):
UDP is defined as the joining or participating in the activities of an organization by an FBI asset or employee without disclosure of FBI affiliation, but not including participation with the knowledge and approval of an official of the organization authorized to act in relation to the activities in question, attendance at an activity open to the public or to acknowledged U.S. Government employees, personal activities not related to FBI employment, or attendance at an academic institution to obtain education or training relevant to FBI employment or to a future undercover role. The UDP policy contained in this Manual applies to investigations conducted pursuant to the NSIG.

Executive Order 12333, Part 2.9, (EO) permits undisclosed participation "in accordance with procedures established by the head of the agency concerned and approved by the Attorney General" The EO provides two substantive requirements. First, UDP must be "essential to achieving lawful purposes," as determined by the agency head, i.e., the Director of the FBI. Second, UDP cannot be undertaken for the purpose of influencing the activity of the organization or its members, unless undertaken on behalf of the FBI in the course of a lawful investigation, or the organization concerned is composed primarily of individuals who are not U.S. Persons and is reasonably believed to be acting on behalf of a foreign power.
a. It should be noted that not all UDP constitutes an undercover operation. Similarly, approvals for UDP do not alleviate the need for review of undercover activities by the undercover review committees.

b. "Organization" refers generally to any association of two or more persons and is to be interpreted broadly.

c. The "participant" in UDP may be a special agent or other employee of the FBI, or a source recruited for the purpose of obtaining information.

(S)

b1
Referral/Consult

b1
Referral/Consult

(S)

5. Undercover Operations (UC): (*Discussed in Section 28*)

b7E

b. Group II UC operations

i. APPROVAL AUTHORITY FOR UDP IN NATIONAL SECURITY INVESTIGATIONS:

b7E

[redacted]

b7E

ii. CRITERIA FOR APPROVAL OF UDP

[redacted]

b7E

7. Mail Cover

i. A "mail cover" is the recording of data appearing on the outside cover of sealed mail matter or of the contents of any unsealed class of mail. A "recording" is a transcription, photograph, photocopy of any other facsimile of the image of the outside cover, envelope, wrappers, or contents of any class of mail. Mail covers are governed by United States Postal Regulations. (See 39 CFR § 233.3)

ii. A request for a national security mail cover [redacted] (See Section Mail Cover at 2-21) b7E

8. Physical and Photographic Surveillance (where such surveillance does not require unconsented entry). This technique includes the use of such surveillance to identify an individual in contact with the subject of a PI. Such surveillance must be approved by the SAC or SAC's designee (ASAC or national security squad supervisor). (See Section 2-09)

9. Video Surveillance of areas which would not require a warrant for law enforcement purposes. When approved by the SAC, the FBI may surveil open public areas where there is no reasonable expectation of privacy. (See Section 2-09)

10. Physical Searches of personal or real property under circumstances in which a warrant would not be required for law enforcement purposes and in which there is no reasonable expectation of privacy (e.g., trash cover. Such physical searches require approval) may be approved by the SAC or the SAC's designee (ASAC or national security squad supervisor may approve).

11. Closed circuit television (CCTV), direction finders, and other monitoring devices under circumstances in which there is no reasonable expectation of privacy and a warrant would not be required for law enforcement purposes (non-trespassory access). Such techniques may be approved by the SAC or ASAC, with CDC or Office of General Counsel review. (See Electronic Surveillance Section for guidance on use of techniques where Privacy Issues attach.)

12. Consensual monitoring of communications (to include consensual computer monitoring). Monitoring of communications to which one of the participants is a consenting party may be approved by SAC or ASAC, with CDC or Office of General Counsel review.

13. Polygraph examinations (See MIOG Part II § 13-22 for policy)

14. National Security Letters (NSL). An NSL is an administrative demand for documents or records which can be made by the FBI in support of national security investigations. There are presently three statutory categories (financial institution records, consumer credit agency records, and electronic communication service provider records) with seven variations of these three NSL types:

[redacted] b7E

15. Accessing stored wire and electronic communications and transactional records in conformity with chapter 121 of Title 18, U.S.C. § 2701-2712.

16. Use of pen registers and trap and trace devices in conformance with Title 50, U.S.C. §§ 1841 - 1846 (FISA), or Title 18, U.S.C. §§ 3121 –3127 (Criminal).

17. Obtaining business records and other tangible things in conformity with Title 50, U.S.C. §§ 1861 - 1863 (FISA).

18. Use of federal grand jury subpoenas and other subpoena authority as may be permitted by law (to include administrative subpoenas where applicable).

2-05 (U) SUMMARY GUIDANCE AND APPLICATION FOR FULL INVESTIGATIONS (FI)

(S)

[redacted]

b1

B. (X) Approval of Full Investigations

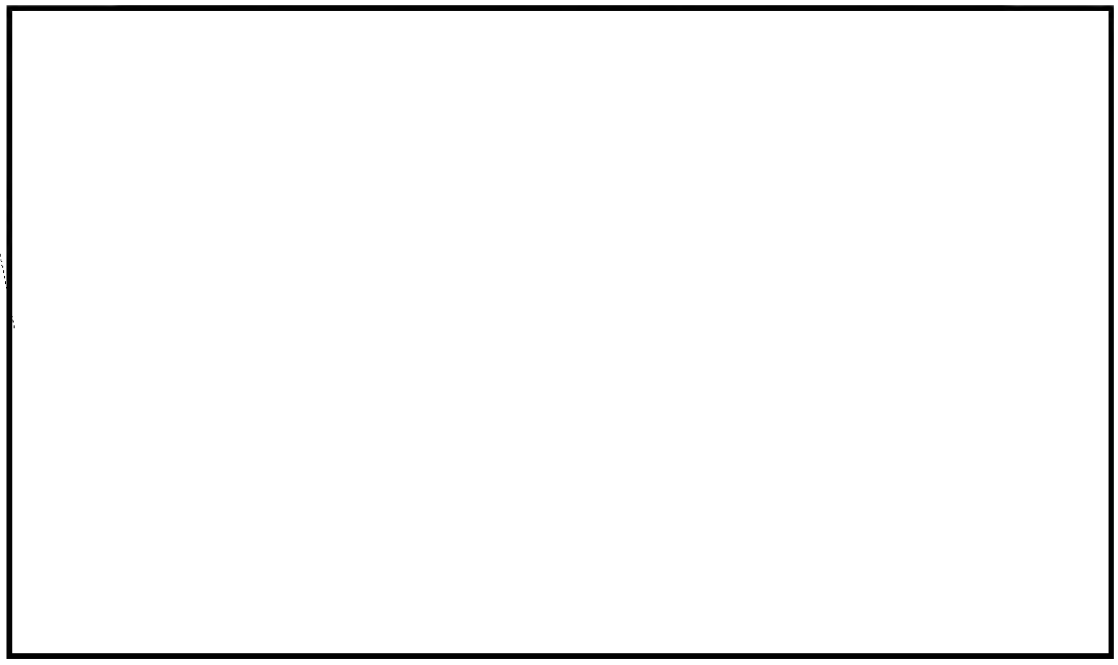
1. An FI initiated by a field office that involves a sensitive national security matter may be approved by an SAC.

b7E

a. *A Sensitive National Security Matter as defined in the NSIG is a threat to the national security involving*

[redacted]

(S)



b1

2-06 (U) Collection of Foreign Intelligence

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-07 (U) Codewords

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-08 (U) Office of Origin

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-09 (U) Physical and Photographic Surveillances

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-10 (U) Interviews In National Security Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-11 (U) Educational Records (Buckley Amendment)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-12 (U) Polygraph Examinations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-13 (U) Hypnosis

A. (U) See: id. Part II, Section 10-12.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

(MIOG Part 2, Section 10-12 For your information.)

10-12 USE OF HYPNOSIS AS AN INVESTIGATIVE AID

10-12.1 Approval to Utilize (See MIOG, Part 2, 10-3.)

Hypnosis is legally permissible when used as an investigative aid for lead purposes in Bureau cases where witnesses or victims are willing to undergo such an interview. The use of hypnosis should be confined to selective Bureau cases. Upon finding a willing witness or victim, Bureau authority must be obtained from the appropriate Assistant Director (AD) responsible for either the Criminal Investigative Division (CID), the Counterterrorism Division (CTD), or the Counterintelligence Division (CD), who may delegate this

authority to their Section Chief designee. The Critical Incident Response Group's (CIRG's) Behavioral Analysis Unit (BAU) functions as a technical resource to the field and must receive copies of all communications pertaining to the use of hypnosis. Set forth in your request for authorization the name of the hypnosis expert you intend to use and a brief summary of the expert's qualifications. You should consider using a psychiatrist, psychologist, physician, or dentist who is qualified as a hypnotist. Those with forensic training are preferred. If there are no qualified or reliable hypnotists available, the BAU should be contacted to obtain the name of a qualified hypnotist nearest your field division. Upon receipt of Bureau authority, the matter must be thoroughly discussed with the USA. Include the fact that the case Agent or the SAC's designee will attend the hypnotic session, and advise whether that person is likely to participate in the hypnotic session. The use of hypnosis on a witness must have the concurrence of the Assistant United States Attorney (AUSA) in that district, as well as the approval of the AD, CID, CTD, or CD, as appropriate, or their substantive Section Chief designee. You are cautioned that under no circumstances will Bureau personnel participate in hypnotic interviews in non-Bureau cases.

10-12.2 Hypnotic Session

(1) It is recommended that written permission (FD-870) to conduct a hypnotic interview be obtained prior to the interview. This permission should include permission of the witness or victim to have the entire hypnosis session audio or video taped or both.
(2) It is important that you either audio or video tape the entire session and any subsequent hypnotic sessions. Video tape, however, is the preferred method of recording these sessions.
(3) When considering the use of hypnosis, one important aspect is the proper prehypnotic explanation of this technique to the witness or victim. Hypnosis is not a product of the power or magic of the hypnotist. The witness or victim is not likely to reveal his or her innermost secrets or lose control of his or her mind. Further, hypnosis itself is not likely to produce any physical or psychological damage to the person hypnotized.
(4) You must also bear in mind that the use of the information obtained through hypnosis cannot be assumed to be necessarily accurate. Careful investigation is needed to verify the accuracy of information obtained during these sessions.

10-12.3 Role of Case Agent in Hypnotic Session

The case Agent will act as liaison with the hypnotist and will attend the hypnotic session. If the case Agent cannot attend, an SAC-approved designee will handle the duties of the case Agent. It must be clearly understood that the hypnotist is charged with the responsibilities of conducting and supervising the hypnotic session, and must remain physically present throughout the proceedings. With the PRIOR CONCURRENCE AND GUIDANCE of the hypnotist, the case Agent may question the witness or victim under hypnosis, but will not conduct the hypnotic induction or terminate the hypnotic state. The request for authorization to utilize hypnosis will include the name of the case Agent or designee who is acting as liaison. The number of persons actually present at the hypnotic session should be held to a minimum.

10-12.4 Hypnosis Evaluation

In order to evaluate the efficacy of this technique, a detailed summary describing the results of the hypnotic interview must be forwarded to the Bureau with a copy to the Critical Incident Response Group's (CIRG's) Behavioral Analysis Unit (BAU). This summary should specifically include the following items:
(1) The identification of any significant investigative information obtained through the utilization of this technique.
(2) Total number of hypnosis sessions to include the length of each session.

(3) The hypnotic technique utilized to include the manner of recording the interview.
(4) The identity of the case Agent or SAC designee and the hypnotist.
(5) Disposition of the case.

2-14 (U) [redacted]

b7E

Superseded by Corporate olicy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-15 (U) Physical Searches in Which a Warrant is Not Required (Trash Covers)

Superseded by the Domestic Investigations and Operations Guide (DIOG), Section 11.4, dated 12/16/2008

Eff. Date: 12/16/2008

2-16 (U) Monitoring Devices Which Do Not Impose Upon Reasonable Expectations of Privacy

(S) [redacted]

b1

2. Field Office authorization for the use and deployment of these devices may be approved by the SAC or ASAC overseeing National Security Investigations.

C. For circumstances in which there exists a Reasonable Expectation of Privacy and a warrant would be required for law enforcement purposes, see the Electronic Surveillance Section of this manual as it pertains to FISA and Title III electronic surveillance.

2-17 (U) National Security Letters (NSL)

Superseded by the Domestic Investigations and Operations Guide (DIOG), Sections 11.9 and 11.9.3, dated 12/16/2008, and by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

2-18 (U) Deleted

2-19 (U) Business Records

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-20 (U) Deleted

(U) 2-21 ~~(S)~~ Mail Covers

Superseded by the Domestic Investigations and Operations Guide (DIOG), Section 11.3, dated 12/16/2008

Eff. Date: 12/16/2008

2-22 (U) Operations Conducted Outside the United States, the CIA MOU

Superseded by Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-23 (U) The Role of Legal Attaches in Foreign Counterintelligence, Foreign Intelligence and Counterterrorism Investigations (See Legal Attache Manual, Part 1, 6-5.2.2.)

Superseded by Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-24 (U) Otherwise Illegal Activities

A. (U) Otherwise Illegal Activities are actions of FBI employees and Assets which would constitute crimes under Federal, State or local law, but for the fact that they have been officially authorized.

B. (U) Activities which, though illegal, neither violate Federal law nor constitute felonies or serious crimes under State or local law, may be approved by SACs, if the activities are necessary to:

[redacted] b7E

3. Prevent or avoid physical injury to individuals or serious damage to property.

C. (U) All other illegal activities must be approved by FBI Headquarters and, if appropriate the FBI's National Security Undercover Review Committee, after consultation with DOJ's OIPR and the Criminal Division, and the concurrence of the Assistant Attorney General, Criminal Division, or his/her designee.

1. Planned or reasonably foreseeable illegal activities must be approved in advance.

2. In emergency situations however (e.g., when illegal activities are required to prevent death, serious injury, extensive property damage, the loss of significant intelligence information or the compromise of an intelligence operation), senior FBI Headquarters officials may approve them. Under such circumstances, though, the aforestated referrals must be made as soon as possible after the fact. See: Attorney General Procedure for Reporting and Use of Information Concerning Violations of Law and Authorization for Participation in Otherwise Illegal Activity in FBI Foreign Intelligence, CI or IT Intelligence Investigations, Section VII.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

(S) [redacted] b1

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-26 (U) Visa Objections

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-27 (U) Office of Foreign Missions (OFM)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-28 (U) National Counterintelligence Executive

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-29 (U) Laboratory Assistance

For information regarding the FBI's Laboratory Division and their variety of services, see Laboratory Division's website: [redacted] b7E

2-30 (U) Monitoring of Establishments Program

(S) [redacted] b1

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: ~~Secret~~

2-31 (U) Purchases of Technical Equipment Program

(S) [redacted] b1

(S) [redacted] b1

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: ~~Secret~~

2-32 (U) Blind Faith Program

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

(C) [redacted] b1

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-34 (U) Special Surveillance Group (SSG) Program

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-35 (U) The Behavioral Analysis Program (BAP)

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-36 (U) Investigations of Current and Former Department of State Personnel, and Diplomatic Missions Personnel Abroad

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-37 (U) Investigations of Current and Former Central Intelligence Agency Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-38 (U) Investigations of Current and Former Military and Civilian Department of Defense Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-39 (U) Investigations of Current and Former Department of Energy Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-40 (U) Investigations of Other Government Agency Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-41 (U) Investigations of White House Personnel

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-42 (U) Investigations of Presidential Appointees

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-43 (U) Investigations of Members of the Judiciary

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-44 (U) Investigations of Members of the U.S. Congress and their Staffs

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-45 (U) Disseminating Information to Other Agencies in the Federal Government

The following guidance is derived from Section VII. B. of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection of October 31, 2003 ("NSIG"), and it pertains to information obtained under the NSIG. Separate rules apply to information obtained under the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations of May 30, 2002. In addition to the following guidance, it is important to bear in mind that information obtained under the Foreign Intelligence Surveillance Act may only be disseminated in accordance with applicable minimization procedures (See Section 3-06 of this Manual).

Legal rules and Department of Justice policies regarding information sharing and interagency coordination have been significantly modified since the September 11, 2001, terrorist attack by statutory reforms and new Attorney General guidelines. The general principle reflected in current laws and policies is that information should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to the national security, except as limited by specific constraints on such sharing. Under this general principle, the FBI shall provide information expeditiously to other agencies in the Intelligence Community, so that these agencies can take action in a timely manner to protect the national security in accordance with their lawful functions. This Subpart provides standards and procedures for the sharing and dissemination of information obtained in national security investigations, foreign intelligence collection, and other activities under the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection of October 31, 2003 ("NSIG") (U)

1. General (U) outside U.S.

a. Information may be disseminated with the consent of the person whom the information concerns, or where necessary to protect life or property from

threatened force or violence, otherwise necessary for the safety or security of persons or property or for the prevention of crime, or necessary to obtain information for the conduct of a lawful investigation by the FBI. (U)

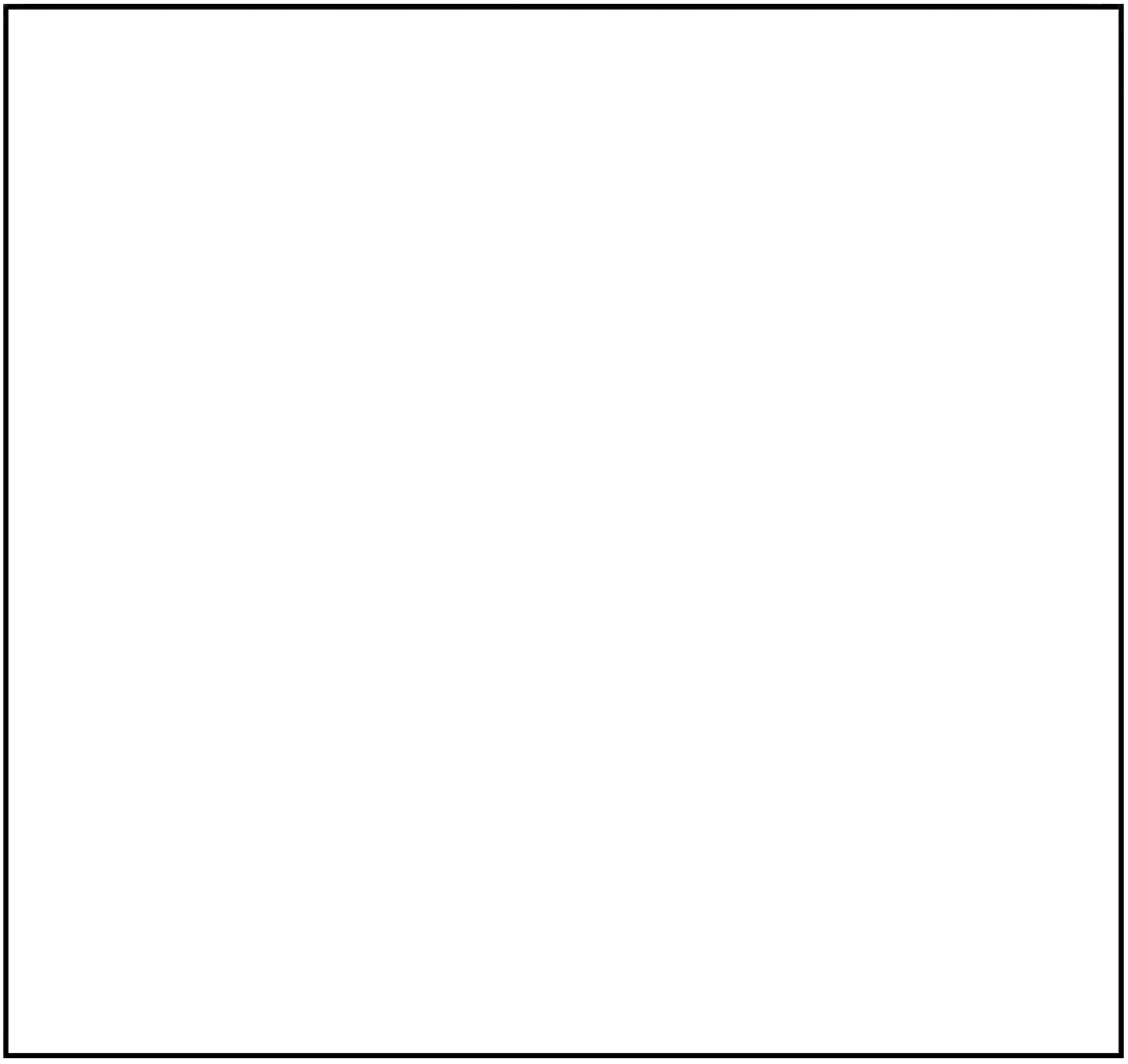
b. Information that is publicly available or does not identify United States persons may be disseminated for any lawful purpose. (U)

c. Dissemination of information provided to the FBI by other Intelligence Community agencies is subject to applicable agreements and understandings with such agencies concerning the dissemination of such information. (U)

b7E
Referral/Consult

2. Department of Justice (U)

a. The FBI may share information obtained through activities under the NSIG with other components of the Department of Justice. (U)



[redacted]

4. Federal Authorities (U)

The FBI may disseminate information obtained through activities under the NSIG to other federal authorities when:

a. the information relates to a crime or other violation of law or regulation which falls within the recipient's investigative jurisdiction, or the information otherwise relates to the recipient's authorized responsibilities;

b. the recipient is a component of the Intelligence Community, and the information is provided to allow the recipient to determine whether the information is relevant to its responsibilities and can be retained or used;

c. the information is required to be furnished to another federal agency by Executive Order 10450 or its successor; or

d. the information is required to be disseminated by statute, Presidential directive, National Security Council directive, Attorney General directive, or interagency agreement approved by the Attorney General. (U)

b7E

2-46 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-47 (U) Disseminating Information to Congressional Committees

A. (U) Members of Congress do not require a determination of eligibility for access to classified information. All other Legislative personnel, however, must be determined eligible by the DOJ Security Officer. See: 28 Code of Federal Regulations Section 17.46(c).

B. (U) Except for briefings and testimony on matters of general intelligence interest, information obtained through activities under the NSIG may be disseminated to the appropriate congressional committees when authorized by the AG or DAG or an official designated by the AG. Other agencies involved in the collection of information will be consulted prior to dissemination to congressional committees. If U.S. person information is to be withheld from dissemination, any decision regarding conflicts over the decision to withhold the information will be referred to the AG, the DAG, or an official designated by the AG for resolution . See Attorney General Guidelines for FBI National Security Investigations Part VII.B.7.

2-48 (U) Disseminating Information to the Federal Judiciary

A. (U) Justices of the U.S. Supreme Court, and Judges of the U.S. Courts of Appeal and District Courts do not require a determination of eligibility for access to classified information. Federal Magistrate Judges and all other Judicial personnel, however, must be determined eligible by the DOJ Security Officer. See: 28 Code of Federal Regulations Section 17.46(c).

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-49 (U) Disseminating Information to the White House

A. Information may be shared with the White House (President, Vice President, Assistant to the President for National Security Affairs, the National Security Council, and Homeland Security Council) when (See Attorney General Guidelines for FBI National Security Investigations Part VII.B.8.):

a. Requested by the National Security Council (NSC)

[redacted]

b7E

d. The limitations on dissemination of information by the FBI to the White House under the NSIG do not apply to dissemination to the White House of information acquired in the course of an FBI investigation

requested by theWhite House into the background of a potential employee or appointee, or responses to requests from the White House under Executive Order 10450.

2-50 (U) Disseminating Information to Foreign Governments, and Investigations at their Behest

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-51 (U) Disseminating Information to State and Local Government Agencies

A. (U) Information relating to crimes may be disseminated to State and local governments with appropriate jurisdiction, if such dissemination is consistent with U.S. National Security interests. See: id. Section VII.B.2.b.

1. Information disseminated to State and local government agencies must include statements that the information may be used for evidentiary purposes only with the express written approval of DOJ, after consultation with the FBI.

B. (U) Classified information may not be disseminated to representative of State or local government agencies unless it can be ascertained that they possess appropriate security clearances and have a proper need-to-know. See: Manual of Administrative Operations and Procedures, Section 9-3.1.3.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-52 (U) Disseminating Information to the Private Sector

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-53 (U) Data Collection Method for Foreign Counterintelligence, Foreign Intelligence and

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 8/9/2010.

Eff. Date: 8/9/2010

2-54 (U) IIIA (Integrated Intelligence Information Application)

b7E

[redacted]

2-55 (U) President's Foreign Intelligence Advisory Board Matters

A. (U) The PFIAB is a body of not more than 16 persons who are not employed by the Government, who are appointed by the President, and who are charged with assessing the quality and adequacy of: (a) intelligence collection, (b) intelligence analyses and estimates, and of (c) foreign counterintelligence and other intelligence activities. It is authorized to review the performance of all agencies within the U.S. Intelligence Community. See: Executive Order 12863, Section 1.2.

1. The PFIAB reports directly to the President; and, to the extent permitted by law, the heads of agencies within the U.S. Intelligence Community must provide it access to all information which it considers necessary for carrying out its responsibilities. See: id. Sections 1.2 and 1.3.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

2-56 (U) Intelligence Oversight Board Matters (Case Identification Number 278-HQ-C1229736-VIO)

Superseded by Corporate Policy Directive #0188D titled, "(U) Guidance on Intelligence Oversight Board Matters," dated 04/22/2009.

Effective Date: 04/22/2009

2-57 (U) Alpha Designations

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 4
Page 4 ~ b1
Page 11 ~ b1
Page 12 ~ b1
Page 24 ~ b7E, Referral/Consult

NFIPM Section 3 (U) Electronic Surveillances and Unconsented Physical Searches

Section 3-01 (U) Consensual Monitoring

Superseded by the Domestic Investigations and Operations Guide (DIOG), Section 11.5, dated 12/16/2008

Eff. Date: 12/16/2008

Section 3-02 (U) Volunteered Tape Recordings

A. (U) Volunteered non-FBI ELSUR recordings should be retained for reasonable periods of time. Their receipt should be documented in case files.
B. (U) If determined to be non-relevant to FBI concerns, contributors should be requested to retrieve them within specified reasonable periods of time. If not retrieved, they may be destroyed.
C. (U) The disposition of volunteered tape recordings should be appropriately documented (e.g., via FD-597s and FD-192s).

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 3-03 (U) DELETED

Section 3-04 (U) Pen Register and Trap and Trace Use

Superseded by the Domestic Investigations and Operations Guide (DIOG), Sections 11.11 and 11.12, dated 12/16/2008

Eff. Date: 12/16/2008

Section 3-05 (U) Unconsented Electronic Surveillances

A. (U) The following requirements pertain to the acquisition, retention and dissemination of nonpublicly available communications and other information resulting from electronic surveillance (ELSUR) on foreign powers, and USPER and non-USPER agents of foreign powers.

(S)

b1

(S) [redacted] b1

Section 3-06 (U) Electronic Surveillance Minimization, Logs and Indexing

Superseded by Corporate Policy Directive #0137D, titled "(S) Standard Minimization Procedures Implementation Policy", dated 11/01/2008.

Eff. Date: 11/01/2008

Section 3-07 (U) Destruction of National Security Electronic Surveillance Recording Media

A. ELSUR Disposition forms
1. FD 986 Disposition of Consensual Monitoring Electronic Surveillance (ELSUR) Media Acquired in Criminal Investigations [redacted]
2. FD-987 Disposition of Foreign Intelligence Electronic Surveillance (ELSUR) Media ([redacted] and b7E
3. FD-989 Volunteered/Subpoenaed Media Pertaining to Criminal/Noncriminal Matters ([redacted] have been developed to cover the following ELSUR media:)
4. FD-988 Title III (FD) Court - ordered wiretaps
B. The legal destruction of no longer needed ELSUR media may be undertaken when certain conditions have been met:
1. General Destruction Guidelines (Excludes Volunteered Media)
a. The following statutory/regulatory requirements must be met in determining destruction eligibility for all original FBI generated ELSUR media:
i. A minimum period of [redacted] must have elapsed from the date the media was intercepted or in Title III investigations [redacted] from the date the media was last sealed by the court. b7E
ii. Media must have no known historical value, i.e., well known public figure(s) or events, etc.)
iii. Media containing evidence of a criminal offense will be retained until a decision is rendered by prosecutory authorities. If they decide to prosecute, media will be retained until the end of the prosecution and appeal processes.
iv. Media required to be retained by any other legal rules or judicial orders will be retained in accordance with the requirements of that law or order. Furthermore, FBI policy requires that the following conditions be satisfied in determining destruction eligibility for all original FBI generated ELSUR media.
v. There are no pending fugitive issues.
vi. There are no pending or anticipated litigation/prosecutorial issues.
vii Regarding Title III investigations, a minimum of [redacted] from receipt of the notice of inventory has passed. (See 18, USC, 2520(e)and 18, USC, 2518(8)(d))
viii The media must no longer have investigative or intelligence value. b7E
ix Regarding Title III and Consensual monitoring in criminal investigations, the case must be in a closed status.
b. Copies of the FBI-generated ELSUR media that are created for convenience or reference are not Federal records and are not subject to the mandatory retention [redacted] This holds as well for copies of FBI-generated ELSUR media that are uploaded into searchable databases,

such as for data-mining purposes. As soon as it is determined that copies are not of operational value and no longer serve a purpose to the office they may be destroyed. With respect to mandatory destruction, reasonable efforts should be made to destroy all copies of FBI generated ELSUR media no later than the date the original is destroyed. Databases composed solely of copies of media, and which are no longer in use, should be reviewed for destruction in their entirety no later than [redacted] from the date they were received. b7E

2. Destruction Guidelines for Volunteered Media (non-FBI Media)

a. Non-FBI ELSUR media, voluntarily turned over to the FBI by anyone outside the FBI, shall be retained for a reasonable period of time, to be determined by the office in possession of the media. Receipt of such media should be appropriately documented in the case file. When it is determined the media is not of evidentiary value or no longer serves a purpose to the office, a reasonable attempt should be made to return the original to the contributor in those instances where return of the media had been requested or was otherwise anticipated. In such cases, the contributor should be contacted and advised to retrieve the media at the local FBI field office within a specified reasonable period of time. In the event the contributor does not wish to have the media returned, or no effort to retrieve the media has been made within a reasonable period of time, the media may be destroyed. Copies of the volunteered media may be destroyed at any time.

b. RMD, pursuant to the authority vested in it by the Director, has determined that volunteered media is not a Federal record (unlike FBI-generated ELSUR media) and should be managed in accordance with relevant FBI policy and the Federal Rules of Evidence. RMD has included a form for volunteered media.

3 The destruction of eligible ELSUR media is mandatory in order to control the growth of records in offices through the systematic disposition of unneeded records. Therefore, all offices are required to actively utilize the authority provided within to alleviate the overcrowding of older, unneeded ELSUR media throughout FBI offices and reduce potential vulnerabilities to the Bureau resulting from deteriorating and aging media.

4 Procedures for the physical destruction of eligible ELSUR media are provided in the FBI Security Policy Manual, entitled "Destruction of Classified and Sensitive Material" [redacted] Offices can also download copies by accessing the Security Division Intranet website listed under Communications Security Policy. b7E

5. The foregoing notwithstanding:

a. Recorded media containing communications that reasonably appear to be "Brady" material shall be retained as if they contained evidence of crimes;

b. Recorded media containing privileged communications shall be retained until DOJ OIPR orders them to be destroyed.

Section 3-08 (U) Operational Support to the Intelligence Community

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 3-09 (U) Operational Operational Technology Division (OTD) Technical Assistance

Superseded by Corporate Policy Directive #0170D titled [redacted] dated 02/26/2009.

Effective Date: 02/26/2009.

Section 3-10 (U) Operational Operational Technology Division (OTD) Technical Assistance Support to the Intelligence Community

A. (U) OTD The Operational Technology Division provides consultation, equipment and installation support in the following investigative endeavors:

(S) [redacted]

(S)

14. (U) The Science & Technology Law Unit (STLU) of the InvestigativeInvestiative Law Branch (ILB) of the Office of General Counsel is responsible in the first instance for advising OTD on legal issues arising from the design, development, deployment and use of OTD capabilities in both classified and non-classified investigations.

(S)

Referral/Consult
b1

(S)

[redacted]

Section 3-11 (U) Unconsented Physical Searches

Superseded by multiple sections in the Domestic Investigations and Operations Guide (DIOG), dated 12/16/2008, and Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010,

Section 3-12 (U) Tax Return Information

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 3-13 (U) Searches of Mail Without Consent

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 3-14 (U) Unconsented Physical Search Minimization, Logs and Indexing

A. (U) Information concerning USPERs acquired through unconsented FISA physical searches may only be used in accordance with minimization procedures. See: id. Title 50, U.S.C., Section 1821(4). Therefore, the following procedures have been established as respects the acquisition, retention, and dissemination of nonpublicly available information concerning unconsenting USPERs that is collected in the course of physical searches [redacted] b7E

1. Guidance for U.S. person status is found in the Attorney General's Guidelines for FBI National Security Investigations And Foreign Intelligence Collection, Section I.C. The general presumption is that all parties subjected to unconsented physical searches are assumed to be USPERs, unless reasonable bases exist to conclude otherwise. In on-line investigations if it is not known if the individual is inside or outside the U.S. there is a presumption of non-U.S. person status. If a person is known or believed to be outside the U.S. there is a presumption on non-U.S. person status.
2. Where a physical search authorized and conducted pursuant to Title 50 U.S.C., Section 1824 involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search. (See: Title 50, U.S.C., Section 1825 (b).
3. Physical searches may include: inspection; examination; reproduction; temporary removal; marking for identification; alteration; substitution or seizure of information, materials and properties which are located in the premises or properties which are authorized for search.

[redacted] b7E

a) This does not limit the collection of information which may involve the conduct of criminal activities.
5. Permanent written logs of items searched must be retained.

[redacted] b7E

6. Should it become apparent during the course of a search of a targeted premises or property that the searched information, material or property contains a communication between a person and an attorney who is representing that person in a matter under indictment, the information, material or property must be: placed under seal, DOJ's OIPR notified, and an appropriate notation entered in the log.
7. All other information, materials and properties containing communications between persons and their attorneys [redacted] may be retained.
a) Such information may be disseminated [redacted] b7E

b) Such information may be disseminated [redacted]

8. The logged identities of USPERs may be indexed into the General Indices [redacted]

9. Information, material or properties which are acquired during the course of FISA physical searches, which concern USPERs [redacted] which do contain evidence of criminal activities, may only be used for law enforcement purposes. b7E

10. Destruction of Records Information obtained by FISA order may be destroyed pursuant to the guidelines set forth in the Attorney General Standard Minimization Procedures (SMP) and the agreement between the FBI and the National Archives, Standard Form 115, signed by the FBI on 3/28/03. SMP provides that records concerning U.S. persons shall be destroyed within a reasonable period (construed as [redacted] except:

a. tapes containing evidence of a criminal offense will be retained until a decision is rendered by prosecutive authorities. If it is decided to prosecute, tapes will be retained until the end of the prosecution process; (U)

b. tapes containing communications that reasonably appear to be exculpatory ("Brady") material shall be retained as if they contained evidence of a crime. (U)

c. tapes concerning privileged communications will be retained until ordered to be destroyed by the Department of Justice, and; (U)

d. tapes required to be retained by rule of law or judicial order will be retained in accordance with the requirements of that rule or order. (U)

In addition, the National Archives would like the FBI to retain information the FBI determines is of historical value.

11. The circumstances and the results of FISA physical searches must be reported to DOJ's OIPR [redacted] b7E

[redacted]

Eff. Date: 08/09/2010 Referral/Consult

Section 3-16 (U) Special Projects Technology for Use in Counterintelligence Division (CD) and Counterterrorism Division (CTD) Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 5
Page 2 ~ b1
Page 3 ~ b1
Page 4 ~ b1
Page 5 ~ b1
Page 6 ~ b1

NFIPM Section 4 (U) The Domain Program and Certain Statute and Treaty Based Investigations

Section 4-01 (U) The Domain Program

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 4-02 (U) Foreign Agents Registration Act (FARA) Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 4-03 (U) Agents of Foreign Governments Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 4-04 Internal Security Act of 1950 Investigations

DELETED – Corporate Policy Office's (CPO) review of NFIPM on 09/24/2010 identified that this is no longer policy.

Section 4-05 (U) Intelligence Identities Protection Act Investigations

A. (U) The Intelligence Identities Protection Act prohibits a person who has authorized access to classified information, which information identifies a covert agent, from intentionally disclosing such information to a person who is not authorized to receive classified information--if it is known that the disclosed information identifies the covert agent; and if it is known that the United States is actively seeking to conceal the agent's intelligence relationship. Criminal penalties attach to violations of this requirement; i.e., a fine of not more than $50,000, and/or a term of imprisonment of not more than ten years. See: Title 50, U.S. Code, Section 421(a).
B. (U) The Act further prohibits a person who, as a result of having authorized access to classified information, from intentionally disclosing information identifying a covert agent to a person who is unauthorized to receive classified information--if it is known that the disclosed information does identify the covert agent; and if it is known that the United States is actively seeking to conceal the agent's intelligence relationship. Criminal penalties attach to violations of

this requirement; i.e., a fine of not more than $25,000 and/or a term of imprisonment of not more than five years. See: id. Section 421(b).

C. (U) And, finally, the Act prohibits a person from disclosing information which identifies a covert agent to any person who is not authorized to receive classified information--if the offender has engaged in a pattern of activities which were intended to expose the agent; if he/she had reason to believe that such activities would impair or impede U.S. foreign intelligence efforts; if he/she knows that the information identifies the agent; and if he/she knows that the United States is actively seeking to conceal the agent's intelligence relationship. Criminal penalties attach to violations of this requirement; i.e.: a fine of not more than $15,000 and/or a term of imprisonment of not more than three years. See: id. Section 421(c).

1. This pertains to a person who, even though he/she does not have access to classified information, seeks to disclose the identity of an agent. Legislative history makes it clear that, in order for such a person to be found guilty, he/she must have consciously sought to identify and expose an undercover intelligence operative, with reason to believe that such conduct would impair U.S. intelligence efforts. See: 128 Congressional Record H2448 (daily ed. May 20, 1982).

D. (U) A covert agent, for purposes of the Act, is:

1. An officer or employee of a U.S. Intelligence Community agency, or a member of the U.S. Armed Forces detailed to such an agency, whose identity as an officer, employee or detailee is classified, and who is serving overseas, or who has served overseas within the last five years; or

2. A U.S. citizen whose intelligence relationship with a U.S. Intelligence Community agency is classified, who resides and acts outside the United States as an Asset to a U.S. Intelligence Community agency, or who at the time of the disclosure, is acting as an FBI Asset; or

3. A non-U.S. citizen whose past or present intelligence relationship is classified, and who is a present or former agent of, or a present or former informant or source of operational assistance to an intelligence agency. See: Title 50, U.S. Code, Section 426(4).

E. (U) It is a defense if the Asset has previously been acknowledged and revealed by the United States; the disclosure is to the Senate Select Committee on Intelligence, or the House Permanent Select Committee on Intelligence; or the person making the disclosure about an Asset is the Asset him/herself. See: id. Section 422.

F. (U) Legislative history indicates that the Act seeks to prevent the activities of persons who are committed to disclosing the identities of multiple covert agents; that is, people who make it their business to ferret out and to publish the identities of agents, "time and time again." The Act is not intended to affect the First Amendment rights of persons who disclose the identities of agents "as an integral part of another enterprise such as news media reporting of intelligence failures or abuses, academic studies of U.S. Government policies and programs, or a private organization's enforcement of its internal rules." See: 128 Congressional Record H2448 (daily ed. May 20, 1982). All investigations under this statute require FBI Headquarters authorization.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 4-06 (U) Registration of Persons Trained in Foreign Espionage Systems Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 4-07 (U) Arms Control Treaty Matter Investigations.

A. (U) Most arms control treaties contain provisions whereby Parties may approve or reject proposed additions to approved treaty inspector lists, in accordance with specific criteria. The FBI participates in this process, by conducting FBI [redacted] and in accordance with each treaty's specific criteria, the FBI may recommend [redacted] Grounds for exclusion vary from treaty to treaty: under the CWC, proposed inspectors may be objected to without explanation; under START, proposed inspectors may be objected to only by virtue of having been indicted or convicted of a criminal offense in the inspected party's territory; or previously expelled by the inspecting party.

1. (U) Military Counterintelligence Service elements' activities are strictly limited with respect to off-base activities, and non-military personnel. Therefore, except for counterintelligence coverage relating to official inspection activities at DOD sites, and sensitive projects (at any locations) over which DOD has overriding proprietary interests, the FBI should never take a secondary role to military counterintelligence.

2. The United States is permitted one designated Portal Perimeter Continuous Monitoring (PPCM) site under the START treaty, located in Votkinsk, Russia. [redacted] b7E

3. In July, 2002 an amendment to the CWCIA exempted the FBI from a mandatory presence at CWC inspection activities at DOD chemical weapons destruction sites.

4. [redacted] is viewed as the primary issue raised by the presence of OPCW inspectors at U.S. commercial chemical facilities. This threat to U.S. confidential business information and trade secrets is potentially significant, as the U.S. chemical industry is the largest in the world. According to the Department of Commerce, the U.S. chemical industry is the United States' largest exporting sector. The threat to U.S. chemical industry confidential business information and trade secrets is greatest from countries with emerging and competing chemical industries, some of whose citizens are employed by the OPCW in various capacities, including as inspectors.

5. [redacted] criminal investigations regarding OPCW inspectors or persons coming into contact with them may be opened under substantive National Foreign Intelligence Program or criminal investigative classifications given the appropriate predications. b7E b7A

6. The short duration of CWC commercial inspections, which are restricted by treaty to 24 to 96 hours, depending on the type of inspection, is likely to limit the scope and duration of FBI investigative activities.

7. Each field office conducting [redacted] is requested to prepare a short summary communication to FBI headquarters under the file number [redacted]

8. Summary communications should be prepared following FBI participation in [redacted] Summary communications should be directed to the CWC Program Manager, FBI Headquarters, under file number [redacted]

B. The Treaty on Open Skies permits States Parties to conduct short-notice aerial observation overflights over the territory of other States Parties. These overflights are conducted in treaty-approved aircraft, equipped with sophisticated optical and video cameras, infrared scanners, and sideways-looking synthetic aperture sensors. Signed in 1992, the treaty has 27 original signatories, and the United States has ratified. The treaty has officially entered into force.

1. During Open Skies flights, signatories utilize treaty-approved observation aircraft and equipment, which are inspected by the inspected State Party prior to use. Inspectors are accompanied on board the aircraft by U.S. military personnel.

2. The United States is obligated to accept up to 42 overflights each year. No single State Party is permitted to use more than 50 per cent of the annual allotment of overflights for any country.

C. The U.S. Government is in the process of evaluating potential counterintelligence issues arising from the adoption of more intrusive verification protocols, and is beginning to carry out training and planning events at potentially inspectable facilities

b7E

D. In 1997, the IAEA Board of Governors adopted additional protocols requiring States Parties to the NPT, including nuclear weapons states, to submit expanded data declarations; to permit IAEA inspectors to take environmental samples to detect the presence of undeclared activities at or near declared nuclear sites; and to permit IAEA inspectors access to any place on a declared nuclear facility. The United States signed the U.S.-IAEA Additional Protocol in 1998; however, it has not yet been ratified. Upon ratification, the United States, as a nuclear weapon state, will voluntarily accept these new measures and provide access as required to declared facilities. The United States may refuse access to locations and information having direct National Security significance.

NFIPM Section 5 (U) [redacted] b7E

Section 5-01 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-02 (U) Countries on the Current National Security List

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-03 (U) Goals and Objectives

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-04 (U) [redacted]

b7E

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-05 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-06 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010. b7E

Eff. Date: 08/09/2010

Section 5-07 (U) [redacted]

(S) [redacted]

(U) B. (X) (Delete) .

(S) [redacted] b1

E. (U) As respects interviews in connection with investigations of diplomatic personnel on temporary assignment, see: id.

(S) [redacted]

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret

Section 5-08 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010. b7E

Eff. Date: 08/09/2010

Section 5-09 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-10 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-11 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-12 (U) [redacted]

b7E

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-13 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-14 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-15 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-16 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-17 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

b7E

Eff. Date: 08/09/2010

Section 5-18 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-19 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-20 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 5-21 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

b7E

Section 5-22 (U)

(S)

b1

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret

Section 5-23 (U) Alpha Designations

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

NFIPM Section 6 (U) Investigations Respecting [redacted] to include [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

Section 7 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

NFIPM Section 8 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

NFIPM Section 9 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

NFIPM Section 11 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website:

[redacted]

Eff. Date: 08/09/2010

NFIPM Section 12 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website:

[redacted]

Eff. Date: 08/09/2010

NFIPM Section 13 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website:

[redacted]

Eff. Date: 08/09/2010

CRT# 1262 Div. CT Cav: SecClass: Unclassified

NFIPM Section 14 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website:

[redacted]

Eff. Date: 08/09/2010

NFIPM Section 15 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

Section 16 (U) Investigations Respecting [redacted]

b7E

Not policy, reference and procedure guide, see Counterintelligence Division's (CD) website: [redacted]

Eff. Date: 08/09/2010

NFIPM Section 18 (U) Issue Threat Investigations

Section 18-01 [redacted] specifically, see: Sections 19 through 26, infra., respectively

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 18-02 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

b7E

Section 18-03 (U) Issue Threat Preliminary Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 18-04 (U) Issue Threat Full Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 18-05 (U) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 18-06 (U) Issue Threat File Numbers

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

NFIPM Section 19 (U) International Terrorism Investigations

(See also MIOG, Part 1, 100-1.2, 100-1.2.2, 100-2.3, 199-1, 256-10, 262-1, 265-1, and 315-1.)

EFFDATE: 04/30/2004 MCRT# 1338 Div. CT Cav: SecClass: Unclassified

Section 19-01 (U) Introduction to International Terrorism Investigations

A. (U) [The 199 (International Terrorism), 265 (Act of Terrorism), 256A (Hostage Taking by International Terrorists), and 262 (Overseas Homicide/Attempted Homicide) classifications have been deleted from the Manual of Investigative Operations and Guidelines (MIOG). The 315 classification (International Terrorism) replaces these four previous violations and will be the appropriate classification for International Terrorism investigations.
B. (U) International Terrorism investigations are national security investigations that support the FBI's priority to protect the United States from terrorist attack. This goal drives the Counterterrorism Division's (CTD's) mission to prevent, disrupt, and defeat terrorist operations before they occur.
C. (U) The nature of International Terrorism investigations must focus on:
1. The complete identification of all subjects.
2. The exhaustive development of intelligence on the operations and capabilities of these subjects, including support, training, recruitment, financing, and attack planning.
3. The dissemination and exploitation of the intelligence, to include human and technical source reporting.
4. A properly targeted response that considers all available investigative opportunities, which includes criminal prosecution. Because of the potential for eventual criminal prosecution, International Terrorism investigations should, whenever possible, be conducted in a manner that preserves this option while collecting disseminable intelligence.
D. (U) Within the international terrorism arena, there is no longer a distinction between "criminal" and "intelligence" investigations, Agents, or squads.
E. (U) There were three significant legal developments after September 11, 2001 that affected International Terrorism investigations:
1. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), effective October 26, 2001.
2. "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," issued on March 6, 2002 by the Department of Justice (DOJ).
3. Foreign Intelligence Surveillance Court of Review's opinion issued on November 18, 2002, In re Sealed Case, 310 F.3d 717 (FISCR 2002).
(U) These developments removed the "walls" that were historically erected between "criminal" and "intelligence" International Terrorism investigations. They also permit unprecedented coordination among the FBI, DOJ, and the U.S. Intelligence Community (USIC).
F. (U) In support of International Terrorism investigations, CTD has developed a Model Counterterrorism Investigative Strategy (MCIS), detailed within this section, which is to be utilized by International Terrorism investigators and analysts.
G. (U) The FBI shall conduct its International Terrorism investigations in compliance with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (National Security Investigations Guidelines, or NSIG), which were issued October 31, 2003. The general objective of the NSIG is the full utilization of all authorities and investigative techniques, consistent with the Constitution and laws of the United States, so as to protect the United States and its people from terrorism and other threats to the national security.

(U) The NSIG permits more aggressive investigation and analysis of international terrorism targets than previously permitted. They authorize three levels of investigative activity in national security investigations: (1) Threat Assessments (TAs), (2) Preliminary Investigations (PIs), and (3) Full Investigations (FIs).
H. (U) In addition to the NSIG, the FBI shall conduct its International Terrorism investigations in compliance with the Constitution, the National Security Act of 1947, 50 U.S.C. 401, et seq.,, and all other applicable statutes, Executive Order 12333 (December 4, 1981) and other Presidential guidance, DOJ regulations and policies, and other Attorney General guidelines.
I. (U) FBI Headquarters will be the national program manager and office of origin for all Foreign Terrorist Organizations designated by the U.S. Secretary of State. Field offices direct investigations on the activities of these organizations only within their respective [areas of responsibility.

EFFDATE: 12/01/2003 MCRT# 1314 Div. CT Cav: SecClass: Unclassified

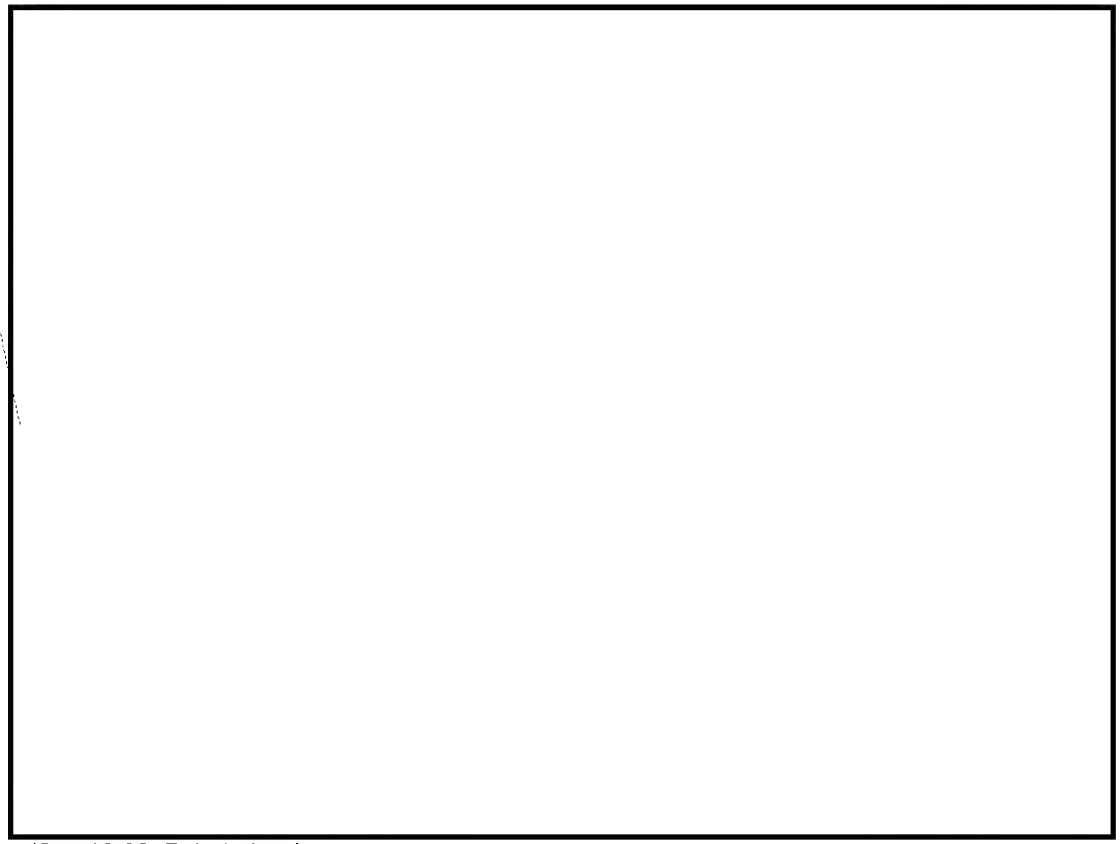
Section 19-02 (U) Investigative Strategy in International Terrorism Investigations

A. (U) The MCIS represents a paradigm shift in how the FBI conducts International Terrorism investigations. Investigators may use a broad array of techniques to aggressively detect, disrupt, and defeat national security threats. The MCIS allows for complete coordination between investigators who may have in the past focused solely on either intelligence collection or criminal prosecution. The MCIS incorporates an ideal that International Terrorism investigations should be conducted in a robust manner and without delay to ensure every logical international terrorism lead is exhaustively pursued.
B. (U) The strategy (or long-term) goal of an International Terrorism investigation is the to develop intelligence regarding all aspects of the terrorist threat. There are several tactical resolutions that can be used in an investigation. Prosecution for a criminal offense is one tactical weapon that can be used in the arsenal available to defeat international terrorism.
C. (U) International Terrorism investigations are nationally managed by CTD. It is essential during the course of each stage of an investigation that field offices coordinate with the appropriate CTD operational, analytical, reports dissemination, and operational support units.

(S)

b1

(S)



b1

(See 19-03, D.1., below.)

(U) 2. (S) Development of the Intelligence/Collection of the Best Evidence In an International Terrorism investigation, field offices should employ all logical investigative techniques permissible for the level of investigative activity being pursued under the NSIG.

a) (U) THREAT ASSESSMENT

(S)

b1

(U) Under this authority, Agents may attend public events and visit public places and conduct surveillance of individuals or groups present in these public settings for the purpose of determining the presence and extent (nature, scope) of a threat to national security. Surveillance may not be conducted for the sole purpose of monitoring the exercise of rights protected by the Constitution.

(U) The retention of information acquired from visits to public places and events is allowed only if it relates to threats to the national security or potential criminal activity.

b) (U) PRELIMINARY INVESTIGATIONS:

(U) (X) Preliminary Investigations are authorized, generally speaking, when there is INFORMATION OR AN ALLEGATION INDICATING THAT A THREAT TO THE NATIONAL SECURITY MAY EXIST. Preliminary Investigations may relate to individuals, groups, organizations, and possible criminal violations.

(S)

b1

(S) [redacted] b1

(U) (S) Counterterrorism-related undercover activities and operations are to be reviewed by and coordinated with the appropriate operational unit and the CTD's Undercover Coordinator.

c) (U) FULL INVESTIGATIONS:

(U) (S) Full Investigations are authorized, generally speaking, when THERE ARE SPECIFIC AND ARTICULABLE FACTS GIVING REASON TO BELIEVE THAT A THREAT TO THE NATIONAL SECURITY MAY EXIST. Like Preliminary Investigations, they may relate to individuals, groups, organizations, and possible criminal violations.

(S) [redacted] b1

[redacted] b7E

(U) (S) An International Terrorism investigation should be treated as an important matter that is pursued in a diligent and thorough manner. Every effort should be made to collect the best possible evidence that can be used to prove any criminal conduct emanating from the international terrorist.

d) (U) CIRCUMSTANCES FOR OPENING A PRELIMINARY OR FULL INVESTIGATION b1

(S) [redacted]

(S) [redacted] b1

e) (U) ANNUAL SUMMARIES
One year after a Full Investigation is authorized and every year thereafter until the Full Investigation is closed, the field office that originated the case shall prepare and provide to CTD a summary of the investigation that includes:
1) The information in Part VII.A.2.a-e of the National Security Investigations Guidelines as it relates to the investigation.
2) An assessment of the extent to which members of the group are aware of the terrorist aims of the international organization.
3) Any sensitive national security matters.
4) Caption, consisting of the subject's name, the character of the case, and the words "Full Investigation."
5) Paragraphs under the following headings: "Office of Origin"; "Date Investigative Summary Prepared"; "Basis for Investigation"; "Investigation to Date"; and "Objective."
6) Name(s) of the subject(s); complete biographical information regarding the subject(s); and information regarding requests for assistance received from foreign law enforcement, intelligence, or security agencies involving USPERs and information on the nature of each such request and whether the requested assistance was furnished or declined.
(U) CTD will forward all such summaries to DOJ's OIPR and Criminal Division. See National Security Investigations Guidelines, Part II.D.4 and Part VII.A.2.

3. (U) Exploitation of the Developed Intelligence

(S) [redacted] b1

(U) (S) In addition to furthering the International Terrorism investigation, investigators need to be mindful of the future analytical importance of collected information. The accumulated intelligence may be compared with other information collected from various government and private sources. The strategic analysis that may be performed with this type of information does not need to be tied to any one particular investigation under the NSIG.

(U) (S) In this regard, it is critical that all international terrorist intelligence information, to include human and technical source reporting, be passed to the appropriate operational unit and the

b7E

[redacted] CTD via electronic means as soon as possible. This includes the results of relevant interviews, crime scene efforts, information received from local and state law enforcement, and all asset and informant data, etc.

4. (U) Execution of a Targeted Response

(S) [redacted]

b1

E. (U) Compliance with the Rule of Law - All International Terrorism investigations will comply with:

1. (U) The National Security Act of 1947, 50 U.S.C. 401, et seq.
2. (U) Executive Order 12,333, "United States Intelligence Activities" (December 4, 1981)
3. (U) The Attorney General's Guidelines for FBI National Security Investigations and Intelligence Collection

EFFDATE: 07/25/2004 MCRT# 1345 Div. CT Cav: SecClass: ~~Secret~~

Section 19-03 (U) Procedural Requirements in International Terrorism Investigations

A. (U) There are three levels of investigative activity outlined in the NSIG for the conduct of International Terrorism investigations: (1) Threat Assessments (TA), (2) Preliminary Investigations (PI), and (3) Full Investigations (FI).

1. (U) An International Terrorism investigation in the [redacted] must be initiated prior to investigative steps being taken by investigative personnel involved in either a Preliminary or Full Investigation.

b7E

(a) All investigative cases on individuals, groups, or organizations in the [redacted] must be characterized as either a Preliminary or Full Investigation. Control files are not investigative cases and thus are not designated as either a Preliminary or Full Investigation. Preliminary investigation initiation dates, and Full Investistigation authorization dates, must be included on all inter-office Electronic Communications. The relevant CTD operational unit must be included on all inter-office communications.

(b) Preliminary Investigations and Full Investigations may relate to individuals, groups, organizations, and possible criminal violations. Since these investigations pertain to threats to

U.S. national security, the notice of initiation must define the known or suspected international terrorism nexus for each individual group, organization or violation.

(c) Preliminary and Full Investigations of groups and organizations should focus on activities related to threats to the national security, not on unrelated First Amendment activities. Any information concerning a group or organization that is relevant to the investigation of a threat to the national security may be sought, including information [redacted] b7E

[redacted]

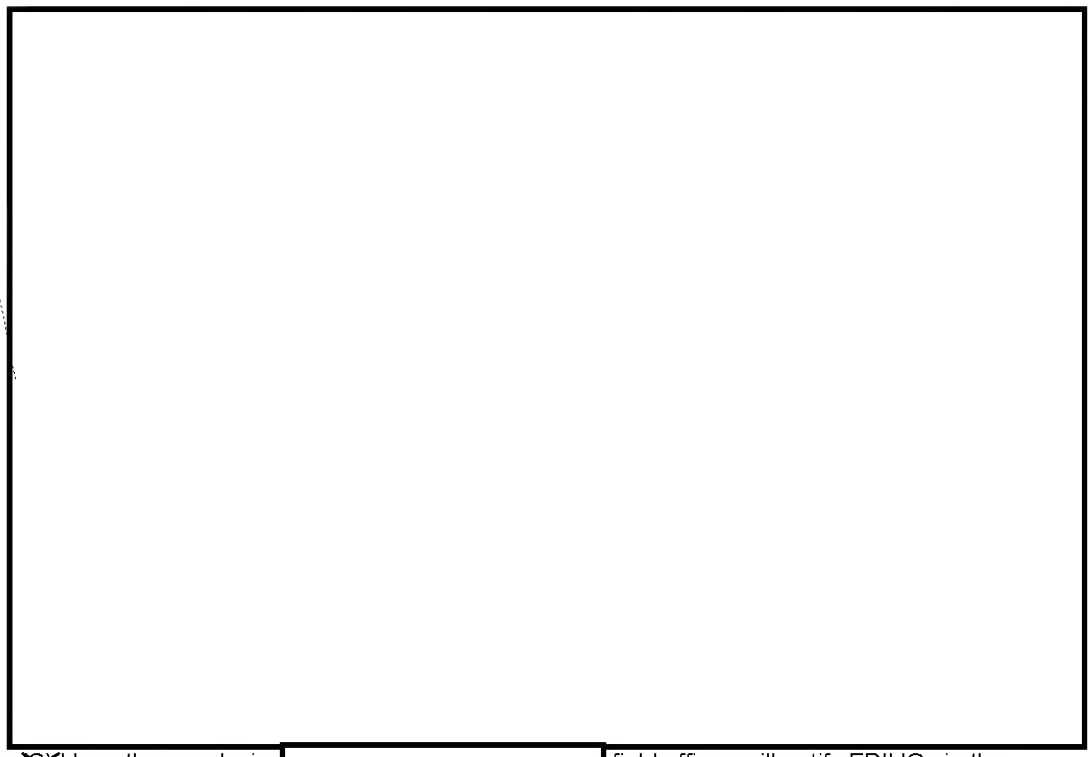
2. (U) Investigative steps taken [redacted] must be documented and uploaded to a control file used as a repository only [redacted]

B. (U) If the available information shows at any point that the threshold standard for a Preliminary Investigation or Full Investigation is satisfied, then that level of investigative activity may be initiated immediately, without progressing through more limited investigative stages.

(U) C. (U) Approval Authority for Opening International Terrorism Investigations.

(S) [redacted] b1

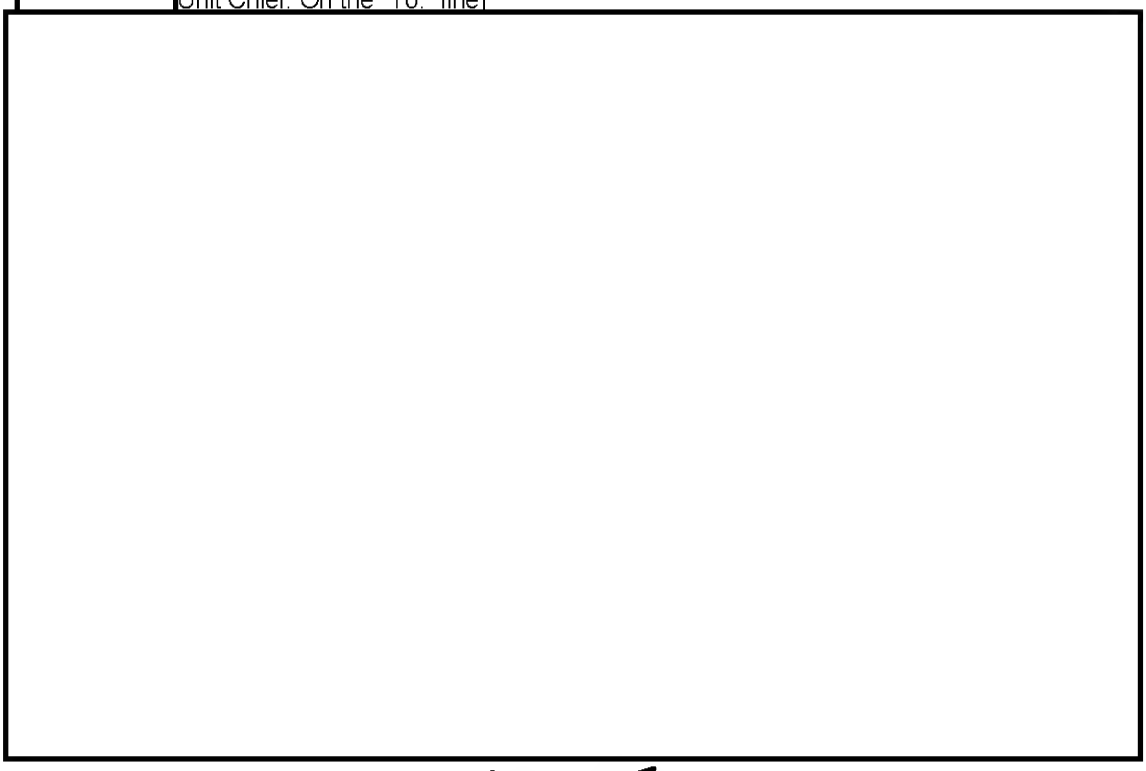
(S)



b1

(U) (S) Upon the conclusion [redacted] field offices will notify FBIHQ via the closing EC which will include both the CTD substantive desk and Counterterrorism, Attention: [redacted] Unit Chief. On the "To:" line]

b7E



b7E

(U) F. (S) Case Characters (See also NFIPM, 1-04.)

(S)

(S)

b1

G. (U) The case opening will be directed as described above in 19-03, D.1.

(U)

(U) If the terrorist affiliation of the subject is unknown, or uncertain the case should initially be classified as openings should be directed to for preliminary review and eventual rerouting if and when a more appropriate substantive unit is identified. Cases designated as should be used only infrequently, and, after consultation they should be reclassified within 90 days.

b7E

(S)

b1

(U) Field office terrorism program managers and supervisors and Legal Attache personnel must stay informed of the various CTD components with operational, analytical, and exploitative responsibility for terrorist groups and the state sponsors of terrorism. One source of information is the CTD website on the FBI Intranet.

(U) An International Terrorism investigation might also impact criminal programs overseen by the Criminal Investigative Division (CID). In those instances, the appropriate CID unit should also be apprised of the investigation in the initial communication to CTD.

(U) Any investigation properly opened as an International Terrorism investigation after delineating specific facts clearly establishing a terrorism nexus, which also possesses a drug nexus, must be conducted not only in conformance with the NSIG, but also in accordance with existing guidelines as stated in MIOG, Part 1, Sections 245 and 281. Since the need for interagency coordination is particularly acute with regard to drug matters, the initial communication advising CTD of the

International Terrorism case initiation must also be directed to the Criminal Investigative Division, Drug Section. If there is an international nexus, then a copy should also be directed to the appropriate Legal Attache for information.

(U) Conversely, if a criminal matter is identified with no discernable or articulated facts indicating a connection to a foreign power, to include international terrorist organizations, then the case should be opened as a criminal matter under CID guidelines and classifications.

H. (U) Case Title Examples

(S)

b1

5. (U) File numbers are unclassified. Case titles, except code word titles, are classified.

b7E

J. (U) Unaddressed Work

1. (U) There will be no unaddressed work within the International Terrorism program of any field office (Reference 66F-HQ-A1308701 Serial 849).

K. (U) Code Word Operations

1. (U) As appropriate, code word operations may be opened as International Terrorism investigations and conducted in accordance with a Preliminary Investigation or Full Investigation.
L. (U) Control and Administrative Files (See MAOP, Part 2, 2-4.1.2 and 2-4.1.5)
1. (U) Control files in the 315 classification (315-FO-C) may be maintained by field offices. Control files are separate files established for the purpose of administering specific phases of an investigative matter or program and would not be considered a PI or FI. They are neither Preliminary nor Full Investigations and thus do not require an annual summary. b7E

[redacted]

M. (U) Subfiles
1. (U) Subfiles should be opened within the International Terrorism investigation in accordance with the standards outlined in MAOP, Part 2, 2-5.1. The list of approved folders, as modified by Virtual Case File, includes:

1A 1A Section exhibits
1B FD-192s (evidentiary bulkies)
1C FD-192s (nonevidence bulkies)
BC Background Information
CE Case Expenditures
ELA ELSUR Administrative
ELA1 ELSUR Original Logs
ELA1A ELSUR Copies and Logs
ELA1B ELSUR Transcripts
GJ Grand Jury Material
FISUR Physical Surveillance Logs
FF Forfeiture Matters
LAB Laboratory/Latent Reports
MC Mail Cover Materials
NC Newspaper Clippings (Press Releases)
SBP Subpoenas
TEL Telephone Subscriber and Toll Information

2. (U) In addition, Subfiles should be opened to organize specific investigative aspects of the case file. These subfiles should be created when information pertinent to the categories arises in the case. These special categories include:
a) FOREIGN Foreign Intelligence,for which permission would need to be granted from a host government prior to release to a third party (for example, the U.S. Attorney's Office).
b) OGA Intelligence from other government agencies, for which permission to disseminate would be required from the originating service (for example, the Naval Criminal Investigative Service). b7E
c) [redacted]
d) CRIMINAL For evidence and other information regarding investigation being pursued relating to specific acts of criminality.
e) FISA ACCURACY. A sub-file must be created and maintained for each FISA application submitted by the case agent containing the materials relied upon to verify the items on the FISA Verification checklist. The sub-file must also contain a "back up" document for each factual assertion contained in the FISA application that is filed with the FISA Court, other than those describing the foreign power. This documentation must be added to the sub-file for each renewal thereafter. Thus, this sub-file will include:

[redacted] b7E

b1
b7E

(S)

O. (U) Classification

1. (U) ACS can only accommodate intelligence up to and including the Secret level. Top Secret intelligence may not be incorporated into ACS. Case File. It is important that investigators properly classify information in terrorism investigations. Classification derives from the sources and methods used to obtain the information, not the actual content of the information. For example, the results of a driver's license check on the subject of a Preliminary Investigation is not classified, since the state department of motor vehicles would likely provide the information on a Law Enforcement Sensitive basis. Similarly, a newspaper article on a subject would not be classified.

b7E

(U) 2. (U) Intelligence received from a foreign government must be marked and handled commensurate with the level of protection the information is accorded by the foreign government providing it. The authorized non-US classification portion abbreviations are:

(TS) for TOP SECRET - NOTE: Top Secret information cannot be uploaded on ACS or sent via [redacted] Use [redacted] to transmit Top Secret information.

(S) for SECRET

(C) for CONFIDENTIAL

(R) for RESTRICTED

(U) for UNCLASSIFIED.

(U) Portion mark foreign government information with FGI plus the ISO 3166 trigraphic country code. ISO 3166 country codes are available on the CAPCO Intelink web site (see capco.dssc.ic.gov).

3. (U) Third Party intelligence, from an agency within the U.S. Intelligence Community, should be sent to the OGA (Other Government Agency) subfile.

4. (U) Situations will often arise when classified information obtained during an International Terrorism investigation will be relevant to a criminal or civil proceeding. In this instance, a declassification review will be required, which, in turn, often requires a more fulsome translation effort than has been previously undertaken. FBI field offices must ensure the declassification review process is coordinated with the National Security Law Branch, Office of the General Counsel, and relevant CTD substantive units. If information was properly classified when placed in the case file, the review process will be much more efficient. If the litigation is a criminal case, further coordination may be required with the Department of Justice Criminal Division and relevant United States Attorney's Offices. Any information that should remain classified, and which is relevant to a criminal proceeding, will be managed under the Classified Information Procedures Act (CIPA). Classified information relevant to a civil proceeding may require a claim of State Secrets, which will require substantial involvement with the Office of the General Counsel, the Civil Division of the Department of Justice, and the personal intervention of the Attorney General (or other relevant Cabinet Officer).

P. (U) The Foreign Intelligence Surveillance Court (FISC)

(S)

[redacted]

b1

Q. (U) Attorney-Client Privilege

(S)

[redacted]

R. (U) Violent Gang and Terrorist Organization File (VGTOF) and Terrorist Screening Center (TSC) Database

1. (U) Subjects of both Preliminary and Full Investigations must be entered into the Violent Gang and Terrorist Organization File (VGTOF) by completing an FD-930. In the FD-930, case Agents must make a recommendation to the Terrorism Review and Examination Unit (TREX) regarding into which databases the subject should be entered and a recommended Handling Code. Upon closing the Preliminary or Full Investigation, the case Agent shall remove subjects who no longer merit inclusion via form FD-930.

2. (U) The "Miscellaneous" field on the FD-930 should include the case Agent's name and 24/7 contact number, the subject's USPER status and country of citizenship, and any other pertinent information. CLASSIFIED INFORMATION MAY NOT BE LISTED IN THE "MISCELLANEOUS" FIELD.

3. (U) The databases into which a subject can be entered will be listed in the FD-930, but they include the Violent Gang and Terrorist Organization File (VGTOF), TSA No Fly or TSA Selectee lists, Treasury Enforcement Communications Systems (TECS), and Consular Lookout and Support System (CLASS) for non-USPERs.

4. (U) The Handling Codes categories, and a description of each, will be listed in the FD-930.

S. (U) Information Sharing

1. (U) Information acquired during the course of an International Terrorism investigation should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to national security, except as limited by specific statutory or policy constraints. Information may be disseminated to obtain information for the conduct of a lawful investigation by the FBI.

2. (U) The FBI (through CTD) shall keep the DOJ Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through the conduct of International Terrorism investigations, except as limited by orders issued by the FISC, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases.
3. (U) Subject to the conditions and terms described in the NSIG, relevant United States Attorney's Offices (USAOs) shall receive information and engage in consultations to the same extent as allowed the DOJ Criminal Division. Thus, the USAOs shall have access to information, shall be kept apprised of information necessary to protect national security and information concerning crimes, shall receive notices of the initiation of investigations and annual summaries, and shall have access to FBI files, to the same extent as the DOJ Criminal Division.
4. (U) Information disseminated to a USAO shall be disseminated only to the United States Attorney (USA) and/or any Assistant United States Attorneys (AUSAs) designated to the DOJ by the USA as points of contact to receive such information. The USA and AUSAs shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. A disseminable LHM is the appropriate method for presenting investigative findings to the Department of Justice. A copy of the LHM must also be directed to the appropriate CTD operational unit.
5. (U) Pursuant to the Attorney General's Intelligence Sharing Procedures, dated March 6, 2002, the FBI must keep a designated AUSA in the relevant USAO fully informed of all relevant foreign intelligence information, as well as evidence of any crime, including information and evidence obtained or derived from FISA, which arises during International Terrorism investigations. Information obtained or derived from FISA shall be marked as required in Title 50, United States Code, Sections 1806(b) and 1825(c).
6. (U) Foreign intelligence is defined in the NSIG as: "information relating to the capabilities, intentions, or activities of foreign powers, organizations, persons, or international terrorist activities."

NEED DEFINITION OF NATIONAL INTELLIGENCE FROM IRTPA

EFFDATE: 07/25/2004 MCRT# 1345 Div. CT Cav: SecClass: ~~Secret~~

Section 19-04 (U) Closing International Terrorism Investigations

A. General
1. Approval for the closing of a Full Investigation may be granted by the SAC or it authorized by the SAC an ASAC with national security responsibility. FBIHQ concurrence is required to close all Full Investigations. The FBIHQ program manager will formally transmit an electronic communication to the field concurring with the case closing. Upon receipt, the field office will provide notification of this closure to all CTD components noted below.
2. Approval for the closing of a Preliminary Investigation may be granted by the SAC or if authorized by the SAC an ASAC with national security investigative responsibility. An information lead to the FBIHQ substantive unit can direct the case remain open for further investigative action. b7E
3. Prior to closing an international terrorism investigation in [redacted] field offices must ensure all reasonable investigative techniques have been exploited. By closing the investigation, the field office is affirming it has exhausted all reasonable and practical intelligence collection methods with respect to the investigation.
4.. If the investigation has uncovered criminal violations of state or federal law, then a declination from the United States Attorney's Office must be received and documented within the investigative case file.

B. Closing Communication to FBIHQ
1. The closing communication will be sent to the Counterterrorism Division to the attention of the following:
a) Substantive unit
b) Terrorist Review and Examination Unit (TREX), LX-1 3S-200
c) CT Analytical Section, LX-1 3W-400
d) TFOS/PMCU, Rm. 4933
e) Other sections or units, as appropriate
f) Appropriate field office or Legal Attaché ("Legat"), if subject relocated
2. An FD-930 will be enclosed to remove or modify the entry in VGTOF.
3. The Details section of the closing communication will contain the following information:
a) The type of investigation (i.e., Preliminary or Full)
b) The date it was opened
c) The date it was converted from a Preliminary Investigation to Full Investigation, if applicable
d) If a Full Investigation, then the date and serial number of the most recent Annual Summary
e) Whether the investigation involves a United States person
f) An assessment of the extent to which the subject is (or members of the group are) aware of the terrorist aims of the foreign power
g) Any Sensitive National Security Matters, which are defined in the NSIG as "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."
h) Name and all aliases of the subject and complete biographical information regarding the subject
i) Subject classification (see D, below)
j) A summary of the investigation to include a list of the investigative techniques used, to include:

[redacted]

b7E

[redacted] b7E

k) Whether the case was submitted to the United States Attorney's Office (for criminal prosecution] and result (indictment or declination); if there is a criminal declination, then the case Agent prepares a letter to the United States Attorney's Office that documents the declination, the letter must be uploaded into the case file, and referenced in the closing communication

l) Reason(s) for closure of case (see C, below)

C. Reason(s) for Closure of Case

b7E Referral/Consult

1. Subject was convicted

a) Include details, to include jurisdiction, statute(s), sentence

2. Subject is incarcerated

a) Include details, to include jurisdiction, statute(s), sentence, incarceration facility, projected release date

b) Incarceration of a subject, by itself, does not meet the basic investigative standard which would merit an international terrorism case to be closed. Factors to be considered prior to closing include, but are not limited to: [redacted]

4. Subject is believed to have moved out of the field office's area of responsibility, but stayed within the USA

a) The office transferring the case may not close its investigation until the receving office has located the subject, opened an investigation, and modified the subject's watch list status via submission of a FD-930 to TREX.

b) include details, to include travel information, traveled with whom, location to which subject moved, and which field office has jurisdiction

c) The change of residence of a subject, by itself, does not meet the basic investigative standard which would merit an IT case to be closed. If a subject has moved outside the area of responsibility of a field office, then the current office of origin will prepare a communication transferring the investigation to the field office covering the subject's new residence. This

communication will summarize the investigation to date and include action leads to both the new field office and the appropriate CTD substantive unit(s) to ensure a seamless and fluid transition between the two field offices.

5. Subject is believed to be deceased

a) Include details, to include basis for belief and circumstances of death

6. Allegations against the subject are without merit

a) Include details

D. Subject Classification

1. Unless the case is being closed due to a finding that allegations against the subject are without merit, provide a characterization of the subject as either an [redacted] and the basis for the classification.

[redacted]

b7E

e) A Recruiter knowingly works to identify and/or attract individuals to participate in terrorism-related activity and/or facilitates those individuals' entry into such activities.
To classify a subject as a Recruiter, investigators must articulate specific information indicating the subject appears to be or could in the near future be expected to knowingly assist a terrorist organization with acquisition of new operatives or supporters.
Examples of information possibly supporting classification of a subject as a Recruiter include: Detainee reporting naming the subject as knowingly assisting the detainee in his entry into terrorist activity and/or training; records or source reporting related to travel arrangements or contacts indicating the subject facilitates others' travel for overseas terrorist training or indoctrination
f) Other: Subjects of counterterrorism investigations who do not otherwise fit the criteria for the above designations. Describe the known or suspected nexus to a foreign power in detail.
E. Completion and Submission of the FD-930, details are available on the TREX website: http://ctd.fbinet.fbi/trex/
1. Completion of Gang, Subgroup, and File # fields
a) In the Gang field, enter International Extremist"
b) In the Subgroup field, enter the VGTOF handling code (1, 2, 3, 4, or silent hit)
c) In the File # field, enter the substantive 315 file number, not an administrative file number (such as the 66 classification) or other control file number
2. To remove or modify a record in VGTOF, send a copy of the closing communication and an enclosed FD-930 to the TREX. Check the "Remove" box or the "Supplements Initial Submission" box at the top of the form. The FD-930 must be sent directly to the TREX, not to the substantive unit.
3. Upon closing a Preliminary or Full Investigation, the case agent shall request the removal from U.S. government watch lists of any subject who no longer merits inclusion.
4. Subjects of Full Investigations may remain in VGTOF and other watchlists, if appropriate. Example: The subject of a Full Investigation is still a threat to national security, but moves to another field office's area of responsibility or outside the USA and thus the field office closes its case. Notify appropriate field office or Legat in the Details area of the closing communication
F. Leads: Field offices are required to provide notification to the appropriate CTD substantive desk whenever an investigation is closed.

EFFDATE: 04/11/2005 MCRT# 1382 Div. CT Cav: SecClass: ~~Secret~~

Section 19-05 (U) Conclusion

A. (U) The FBI's investigation of international terrorism, through the MCIS, emphasizes collecting, analyzing, and disseminating intelligence on terrorist targets in an effort to prevent future attacks. Criminal prosecution remains a possibility throughout the investigation. This approach, which employs both intelligence collection and traditional law enforcement tools, is a central to the FBI's successful counterterrorism mission.

EFFDATE: 12/01/2003 MCRT# 1314 Div. CT Cav: SecClass: Unclassified

Section 19-06 (U) Terrorism Screening Procedures (Watchlisting)

A. (U) Role of the Terrorist Screening Center (TSC)
(U) The TSC was established by Homeland Security Presidential Directive (HSPD) 6 on 09/16/2003, which directed the establishment of an organization that would consolidate the government=s approach to terrorism screening and provide for the appropriate and lawful use of

terrorist information in screening processes. The mission of the TSC is to facilitate and assist in the protection against terrorism by:
1. Consolidating the Government=s approach to terrorism screening;
2. Providing for the appropriate and lawful use of the terrorist information in screening processes;
3. Maintaining consolidated, thorough, accurate and current terrorist identities information;
4. Sharing information globally and between the Federal, State, local, territorial, and tribal law enforcement and intelligence communities; and carrying out these activities in a manner consistent with the Constitution and applicable laws protecting privacy and civil liberties.

B. (U) Watchlisting Policy for Known or Appropriately Suspected Terrorists

1. The Counterterrorism Division's (CTD) policy requires that all main IT subjects for both Full and Preliminary Investigations in the 315 classification and all subjects of domestic terrorism (DT) Full Investigations in the 266 classification shall be nominated for entry into the TSC's Terrorist Screening Database (TSDB) and all eligible supported systems if the subject meets the criteria for inclusion. Individuals being investigated as part of a Threat Assessment shall not be included in the TSDB or any of its supported systems. See Section C below for a discussion of the TSDB's supported systems.
2. Main DT subjects for both Full and Preliminary Investigations in the 174 classification and subjects of DT Preliminary Investigations in the 266 classification may, at the discretion of the nominating official (e.g., Joint Terrorism Task Force, FBI Case Agent or Intelligence Analyst, or Headquarters supervisor, if HQ is the Office of Origin), be nominated for entry into the TSDB and, if the subject meets the criteria for inclusion, all eligible supported systems.
3. The nomination of main subjects for entry into the TSDB and all eligible supported systems is consistent with HSPD-6 and the "Memorandum of Understanding On Integration and Use of Screening Information to Protect Against Terrorism," issued 09/16/2003 (the "MOU"), and provides a consistent and efficient method to ensure that only individuals who are known or appropriately suspected terrorists are included in all eligible supported systems.
4. Subjects with no nexus to terrorism shall not be nominated for entry into the TSDB. Terrorist group or organization names cannot be nominated for entry into the TSDB. The procedure for nominating subjects for entry into the TSDB is detailed below in Section D.

C. (U) Terrorist Screening Database and its Supported Systems

(U) The TSC maintains the U.S. Government's consolidated terrorist watchlist, known as the TSDB, of the names and other identifying information for all known or appropriately suspected terrorists. The TSC consolidated into the TSDB the existing subsets of information about known or appropriately suspected terrorists from supported systems.

(U) The TSC receives "Terrorist Identifiers" (as defined in Addendum B to the aforementioned MOU) from two sources. The information about known or appropriately suspected international terrorists comes from the National Counterterrorism Center (NCTC), which assembles and analyzes information from a wide range of sources. The FBI provides the TSC directly with the identities of known or appropriately suspected purely domestic terrorists. The Terrorist Identifiers in the TSDB are deemed For Official Use Only.

(U) The TSDB and its supported systems are used by Federal, State, local, territorial, and tribal authorities and certain foreign governments to screen for known or appropriately suspected terrorists as part of their security or law enforcement missions. These authorities use their systems to run name checks against TSDB data. The TSC regularly exports updated subsets of TSDB data to the following supported systems:

1. Violent Gang and Terrorist Organization File (VGTOF). VGTOF is a file within the National Crime Information Center (NCIC) database that is composed of information in possession of the U.S. Government related to the identities of individuals known or appropriately suspected to be or have been involved in activities constituting, in preparation for, in aid of, or related to IT or DT.
2. No Fly and Selectee Lists. On 10/21/2004, the Homeland Security Council Deputies Committee met and established the following criteria for the No Fly and Selectee Lists:

No Fly List:

[redacted]

b7E

For additional guidance regarding the implementation of the aforementioned criteria for entry on these two Lists, refer to the No Fly and Selectee List Guidance (dated 07/25/2006) which is available on the FBI Intranet.

[redacted]

D. (U) Nomination of Subjects for Entry into the TSDB and Initial Submission Procedure

1. To nominate a subject to the TSDB, the nominating official (e.g., Joint Terrorism Task Force, FBI Case Agent or Intelligence Analyst, or Headquarters supervisor, if HQ is the Office of Origin) must e-mail the following documents to the Terrorist Review and Examination Unit ("TREX Unit") at HQ_DIV13_TREX:

a) Opening Electronic Communication ("EC"); and

b) FD-930 for each subject who is a known or appropriately suspected terrorist. Use the eForm version of the FD-930 to enter the subject; and

c) Notice of Initiation (NOI) or Letter Head Memo (LHM).

2. An individual watchlisted as a known or appropriately suspected terrorist will be included in all supported systems if the individual meets the criteria for inclusion, unless the justification for exclusion (made in accordance with Section E below), is supported by the TREX Unit and the TSC.

b7D
b7E
Referral/Consult

3. All subjects who qualify for inclusion on the No Fly List will be nominated to that list in no more than 24 hours. Individuals will not be included on the No Fly or Selectee Lists without sufficient derogatory information supporting inclusion.
4. The TSDB contains only the identities of known or appropriately suspected individual terrorists. A nomination to include a subject in the TSDB who is not associated with terrorism will not be processed.
5. The submission of an EC, FD-930 and NOI/LHM affirms the subject is a known or appropriately suspected terrorist. Any FD-930s received without an accompanying EC will not be processed.
6. After the TREX Unit reviews and approves the FD-930, it forwards the FD-930 to NCTC for all IT nominations and directly to the TSC for all purely DT nominations. For IT nominations, NCTC forwards the relevant information to the TSC for entry into the TSDB and eligible supported systems, as appropriate.

E. (U) Exclusion from a Particular Supported System

1. An individual included in the TSDB will be included in all supported systems if the individual meets the criteria for inclusion. An individual may be excluded from a particular supported system in rare cases when there is a reasonable and detailed operational justification for not including the individual in a particular supported system and the request for exclusion has been reviewed and approved by the TREX Unit and the TSC. The reasonable and detailed justification must be included in both the EC and the appropriate field of the FD-930. The existence of a local or state "Sunshine Law" is not sufficient justification for exclusion.
2. The justification to exclude a subject from any particular support system will be reviewed by the TREX Unit and the TSC. After the review, the TREX Unit will notify the nominating official regarding whether CTD: (1) supports the justification resulting in the exclusion of the name from a particular supported system, or (2) finds the justification for exclusion insufficient resulting in the subject's addition to the particular supported system. The TSC will make the final decision.

F. (U) VGTOF Handling Codes

(U) Each record in VGTOF will be assigned a Handling Code, as follows:
1. Handling Code 1 is reserved for individuals for whom there is an active arrest warrant in the NCIC Wanted Persons File. The warrant number must be included on the FD-930. If the arrest warrant is no longer valid, then the case agent has an obligation to submit a new FD-930 to the TREX Unit to update the record. The following banner appears in VGTOF when a Handling Code 1 is encountered:

"WARNING - APPROACH WITH CAUTION
THIS INDIVIDUAL IS ASSOCIATED WITH TERRORISM AND IS THE SUBJECT OF AN ARREST WARRANT, ALTHOUGH THE WARRANT MAY NOT BE RETRIEVABLE VIA THE SEARCHED IDENTIFIERS. IF AN ARREST WARRANT FOR THE INDIVIDUAL IS RETURNED IN YOUR SEARCH OF NCIC, DETAIN THE INDIVIDUAL PURSUANT TO YOUR DEPARTMENT'S PROCEDURES FOR HANDLING AN OUTSTANDING WARRANT, AND IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER AT [redacted] FOR ADDITIONAL DIRECTION. IF AN ARREST WARRANT FOR THE INDIVIDUAL IS NOT RETURNED, USE CAUTION AND IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER [redacted] FOR ADDITIONAL DIRECTION.
IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC."

b7E

2. Handling Code 2 is reserved for individuals for whom DHS has or will issue a ADetainer@ should the individual be encountered by law enforcement.

Nominations of individuals in VGTOF with this handling code will require a particularized review of the intelligence records. To use Handling Code 2, a review and approval for legal sufficiency by both the Chief Division Counsel and the Office of General Counsel (OGC) is required for this Handling Code. The TSC-OGC representative, in coordination with the National Security Law Branch (NSLB), will provide such approval for OGC. The following banner appears in VGTOF when a Handling Code 2 is encountered:

"WARNING -- APPROACH WITH CAUTION
PLEASE DETAIN THIS INDIVIDUAL FOR A REASONABLE AMOUNT OF TIME FOR QUESTIONING. THIS INDIVIDUAL IS OF INVESTIGATIVE INTEREST TO LAW ENFORCEMENT REGARDING ASSOCIATION WITH TERRORISM.
IMMEDIATELY CONTACT THE TERRORIST SCREENING CENTER AT [redacted] FOR ADDITIONAL DIRECTION. b7E
IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC."

3. Handling Code 3 is reserved for those records which contain a full first and last name and a complete date of birth or a full first and last name and a passport number. The following banner appears in VGTOF when a Handling Code 3 is encountered:

DO NOT ALERT THIS INDIVIDUAL TO THIS NOTICE.
THE PERSON QUERIED THROUGH THIS SEARCH MAY BE AN INDIVIDUAL IDENTIFIED BY INTELLIGENCE INFORMATION AS HAVING POSSIBLE TIES WITH TERRORISM.
CONTACT THE TERRORIST SCREENING CENTER AT [redacted] FOR ADDITIONAL IDENTIFYING INFORMATION AVAILABLE TO ASSIST YOU IN MAKING THIS DETERMINATION. b7E
DO NOT ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE OR LOCAL STATUTES. CONDUCT LOGICAL INVESTIGATION USING TECHNIQUES AUTHORIZED IN YOUR JURISDICTION AND ASK PROBING QUESTIONS TO DETERMINE IF THIS INDIVIDUAL IS IDENTICAL TO THE PERSON OF LAW ENFORCEMENT INTEREST.
WARNING -- APPROACH WITH CAUTION.
IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.
DO NOT ADVISE THIS INDIVIDUAL THAT THEY ARE ON A TERRORIST WATCHLIST."

4. Handling Code 4 is reserved for those records which have limited biographical data, but are of interest to law enforcement. The following banner appears in VGTOF when a Handling Code 4 is encountered:

"***DO NOT ALERT THIS INDIVIDUAL TO THIS NOTICE***
THE PERSON QUERIED THROUGH THIS SEARCH MAY BE AN INDIVIDUAL IDENTIFIED BY INTELLIGENCE INFORMATION AS HAVING POSSIBLE TIES WITH TERRORISM.
CONTACT THE TERRORIST SCREENING CENTER AT [redacted] FOR ADDITIONAL IDENTIFYING INFORMATION THAT MAY BE AVAILABLE TO ASSIST YOU IN MAKING THIS DETERMINATION. b7E
DO NOT ARREST THIS INDIVIDUAL UNLESS THERE IS EVIDENCE OF A VIOLATION OF FEDERAL, STATE OR LOCAL STATUTES. ATTEMPT TO OBTAIN SUFFICIENT IDENTIFICATION INFORMATION TO POSITIVELY IDENTIFY THIS INDIVIDUAL IN A MANNER CONSISTENT WITH THE TECHNIQUES AUTHORIZED IN YOUR JURISDICTION.
WARNING - APPROACH WITH CAUTION.
IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.
DO NOT ADVISE THIS INDIVIDUAL THAT HE IS ON A TERRORIST WATCHLIST"

G. (U) Silent Hits

(S) [redacted] b1

(S)

b1

H. (U) U.S. Person (USPER) status
A subject's USPER status does not affect his/her nomination for entry into the TSDB, but it may affect a subject's export to a particular supported system. For example, the TSC exports USPER identities to DOS's CLASS-Passport system, but not to CLASS-Visa, TUSCAN or TACTICS. Since an USPER would have no reason to apply for a visa to enter the United States, USPERs are not in CLASS-Visa.
I. (U) Nomination of Non-FBI Subjects for Terrorist Screening
1. Individuals who are known or appropriately suspected terrorists, but who are not FBI subjects of an IT investigation, may be nominated by the FBI for inclusion in the TSDB via the NCTC as provided below.
2. The FBI may nominate non-USPERs or presumed non-USPERs (as those terms are defined in the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, or NSIG, issued 10/31/2003) who are not subjects of IT investigations (315 classification) for entry into NCTC's Terrorist Identities Datamart Environment (TIDE) for terrorist screening purposes. Such entry does not apply to subjects of pending or closed FBI IT investigations (315 classification). For procedures relating to the nomination of an FBI subject for entry into the TSDB, refer to Section D above.
3. All FBI personnel -- either Headquarters or Field Offices -- desiring to submit information (i.e., military detainee or Legat records) to NCTC for terrorist screening purposes must send an EC, uploaded with unrestricted text, to the substantive unit in CTD that has program management responsibility for the terrorist organization to which the known or appropriately suspected terrorist is a member or affiliate.
4. The EC to CTD should contain enough substantive information to identify the individual as a known or appropriately suspected terrorist. Although the teletype to NCTC will not contain sources and methods, the EC to the substantive desk should include the source of the information. The EC should not provide mere conclusions (e.g., "subject is an international terrorist"). Instead, the EC should provide specific justification (e.g., "subject is a member of a HAMAS cell that includes individuals currently opened as Full Investigations in the 315 classification"). Any information that may be subject to use restrictions (i.e., federal grand jury (Rule 6e), FISA, sealed material or Bank Secrecy Act information) should be clearly marked. When known, information that an individual is considered "Armed & Dangerous" should also be clearly marked.
5. The EC should also contain all the identifying information known on the individual:
a. full legal name and aliases;
b. dates of birth (month, date, and year);
c. places of birth;
d. unique identifying numbers such as alien registration numbers, visa numbers, social security account number(s);
e. passport information, including passport numbers, countries of issuance, dates and locations of issuance, expiration dates, passport photos, and other relevant data;
f. countries of origin and nationalities;
g. physical identifiers, such as sex, race, height, weight, eye color, hair color, scars, marks, or tattoos;
h. known locations, i.e., addresses;
i. photographs or renderings of the individual;
j. fingerprints or other biometric data;
k. employment data;
l. license plate numbers; and
m. any other terrorism information that originators specifically provide for passage to the TSC.

6. The substantive unit will be required to draft a teletype to NCTC requesting the entry of the individual(s) into TIDE. Based on the derogatory information in the teletype, NCTC will determine whether to nominate an individual to the No Fly or Selectee list. For non-subjects, a teletype is required, since this information is being disseminated outside of the FBI to the U.S. Intelligence Community (USIC).
7. Once the teletype is received by NCTC, a record will be generated and the For Official Use Only (FOUO) identifying information will be forwarded to the TSC. The individual will then be entered into the TSDB and eligible supported systems.
8. The teletype to NCTC should not contain any information identifying sources or methods, since this teletype will be available for review by authorized members of the USIC who have access to NCTC Online. However, it should contain all relevant unclassified identifying information referenced above in subsection 5.

J. (U) On-going Requirement to Update Information

(U) After the initial submission of the FD-930, it is essential that information about a known or appropriately suspected terrorist (e.g., change in investigation status, updated biographical information or in the nominating official's contact information) be updated as information changes and/or new information becomes available. To update or modify a record, check the "Add Data to Existing Record" box or the "Modify or Delete Data from Existing Record" box at the top of the FD-930 and enter the updated information in the appropriate fields. The FD-930 and an EC must be sent via e-mail directly to the TREX Unit with a copy to the substantive unit.

K. (U) Removal of Identities from the TSDB

1. To remove an identity from the TSDB and all the eligible supported systems, e-mail a copy of the approved closing communication and FD-930 to the TREX Unit at HQ_DIV13_TREX. The "Administrative" section of the closing communication should include language to the following effect: "Per concurrence with CTD [reference approving authority and substantive unit], the PI/FI is being closed." Check the "Remove Individual From ALL Watchlisting and Supported Systems" box. The FD-930 and EC must be e-mailed directly to the TREX Unit with a copy to the substantive unit. The TREX Unit does not require hard copies of the FD-930 and EC.
2. When a Preliminary Investigation is closed, the subject must be removed from the TSDB (i.e., VGTOF and the other supported systems).
3. If a Full Investigation is closed because no link to terrorism was established, the subject must be removed from the TSDB. However, if a subject of a Full Investigation moves to another Field Office=s jurisdiction or outside the United States, the subject should remain in the TSDB, if the subject continues to pose a threat to national security. In those cases, the case agent must notify the appropriate FBI Field Office or Legat in the closing communication that his/her subject is moving to their jurisdiction.

L. (U) Expedited Nominations

(U) In the event that a subject must be watchlisted in an expeditious manner (e.g., the known or appropriately suspected terrorist's travel is imminent), a nomination may be processed directly by the TSC. This expedited action, known as an Expedited Nomination, ensures the subject's information is sent to TSC's exported data base (i.e., No Fly List, Selectee List, VGTOF, IBIS, CLASS, TUSCAN and TACTICS) for immediate notification. Expedited nominations must still meet the criteria for entry in the TSDB. Most Expedited Nominations will request placement on the Transportation Security Administration's (TSA) No Fly or Selectee List. The TSC will determine if the subject qualifies for either of these lists. In addition to the TSA lists, the expedited nominee should also be placed in VGTOF and IBIS. The DOS's representative at TSC will be notified to determine the necessity and expeditious nature of placing the subject(s) in CLASS and the other supported systems (TACTICS and TUSCAN).

(U) All Expedited Nominations will be processed immediately at TSC, and thereafter the nominations paperwork will be sent to NCTC for IT matters (so that a record in TIDE can be created) or the TREX Unit for DT matters for the nomination process on the next business day. The TSC will remove the expedited record from the TSDB and all supported system 72 hours

later, unless the nominating official forwards sufficient derogatory information through the routine process.
(U) All non-expedited requests will be processed through the normal daily ingest process and should be submitted to the TREX Unit. The TREX Unit will submit to NCTC for IT matters and directly to TSC for purely domestic matters.
M. (U) Arrest Warrants and Interpol Notices for Watchlisted Individuals
If there is an active arrest warrant in the NCIC Wanted Persons File for a subject in the TSDB, then the case agent must submit both a notification EC and FD-930 to the TREX Unit. VGTOF Handling Code 1 is reserved for subjects who have an active arrest warrant in the NCIC Wanted Persons File.
1. The notification EC and FD-930 must include the NCIC Warrant Number listed in the NCIC Wanted Persons File. In the case of currently watchlisted individuals, this documentation should also include any descriptive, biographical, or cautionary information about the subject that has not already been entered into the TSDB. The TREX Unit will enter the information into VGTOF, and, if necessary, make an appropriate change to the subject's handling code.
2. If there is an active arrest warrant for the subject, absent sensitive circumstances, the case agent should apply for an Interpol Red Notice. Interpol publishes these notices to their member states with a view to arrest and extradite the person to the country who holds the arrest warrant. The application for an Interpol Red Notice is available on the FBI's Intranet or by contacting an FBI representative at Interpol's U.S. National Central Bureau in Washington, D.C.
3. If an Interpol Red Notice is filed, then notification must be submitted to the TSC and the appropriate unit at FBIHQ. The Red Notice notification may be included in the original notification EC concerning the arrest warrant, or in a later EC as needed. The TSC will enter into the TSDB that the individual is subject of an Interpol Red Notice.
4. If an arrest warrant is no longer active in the NCIC Wanted Persons File (e.g., the arrest warrant has been served or recalled by the court), then a notification EC must be sent to the TREX Unit. The TREX Unit will make an appropriate entry into VGTOF reflecting the disposition of the warrant.
5. In rare circumstances, such as a sealed indictment, it may be necessary to keep information concerning an arrest warrant out of the TSDB. In such circumstances, the notification EC concerning the warrant must articulate a reasonable and detailed justification for such exclusion.

Section 19-07 (U) Deleted

EFFDATE: 12/01/2003 MCRT# 1314 Div. CT Cav: SecClass: Unclassified

Section 19-08 (U) Deleted

EFFDATE: 12/01/2003 MCRT# 1314 Div. CT Cav: SecClass: Unclassified

Section 19-09 (U) Deleted

EFFDATE: 01/17/2003 MCRT# 1273 Div. CT Cav: SecClass: Unclassified

Section 19-10 (U) Human Rights Offenses

The above deleted text does not pertain specifically to 315 investigations. If its inclusion is necessary in the NFIPM, then it should be moved to a different section that does not deal specifically with 315 investigations.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CT Cav: SecClass: Unclassified

Section 19-11 (U) The Behavioral Analysis Program

A. (U) See: Section 2-35, supra.

b7E

EFFDATE: 04/29/2002 MCRT# 1262 Div. CT Cav: SecClass: Unclassified

Section 19-12 (U

Section 19-13 (U) Alpha Designations

A. (U) See: Section 1-04, supra.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CT Cav: SecClass: Unclassified

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 1
Page 13 ~ b1, b7D, b7E

NFIPM Section 21 (U) Proliferation Investigations

Section 21-01 (U) Proliferation Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 21-02 (U) FBI Headquarters Oversight

A. (U) WMDD's Counterproliferation (CP) Operations Unit is the focal point for all proliferation of WMD matters and has programmatic oversight for WMD CP investigations, i.e., those with the [redacted] designation), facilitates all USIC CP liaisons, and provides strategic, operational and tactical analytic support to Counterintelligence Division's CP operations and investigations while CD's [redacted] exercise administrative oversight for such CP cases. b7E

EFFDATE: WMDD Establishment EC dated 3/16/2006, 319X-HQ-A1487711-CTD, Serial 2

Section 21-03 (S/NF) [redacted]

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

b1

Eff. Date: 08/09/2010

Section 21-04 (S//NF) [redacted]

DELETED – Corporate Policy Office's (CPO) review of NFIPM on 09/24/2010 identified that this is no longer policy.

(U) Section 21-05 (~~S/NF/ORCON~~) FBI [redacted] Program (Formerly the [redacted] Initiative)

b7E

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 21-06 (U) Alpha Designations

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

NFIPM Section 22 (U) Economic Counterintelligence and Economic Espionage Investigations

Section 22-01 (U) Economic Counterintelligence and Economic Espionage Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 22-02 (U) Alpha Designations

NFIP File Classifications and Alpha Designations can be found on the Resource Planning Office's (RPO) FBI Classifications website.

NFIPM Section 23 (U) Threats to the National Information Infrastructure - Counterterrorism/Counterintelligence (TNII - CT/CI) Computer Intrusion (288J and 288B Subclassifications)

(For more information regarding the 288 classification and subclassifications, see EC from Cyber to Records Management dated 11/15/2005, 319W-HQ-A1487698 serial 27.)

Section 23-01 (U) Threats to the National Information Infrastructure (TNII) Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-02 (U) Lead Agencies

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-03 (U) The National Coordinator for Security, Infrastructure Protection and Counterterrorism

A. (U) The National Coordinator participates as a full member of Deputies or Principals Committee meetings when they are convened to consider infrastructure issues; and he/she reports to the President through the Assistant to the President for National Security Affairs.
B. (U) The National Coordinator ensures interagency coordination for policy development and implementation; and he/she chairs the Critical Infrastructure Coordination Group. See: id., Section VI(3) and Annex A, p. 11.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CY Cav: SecClass: Unclassified

Section 23-04 (U) Interagency Groups

A. (U) The National Infrastructure Protection Center (NIPC) serves as the national critical infrastructure threat assessment, warning, vulnerability and law enforcement investigation and response entity. It consists of investigators from Lead Agencies who are experienced in computer crimes and infrastructure protection.
1. In the event of a foreign threat or attack, depending on the nature and level of the threat or attack; protocols established between DOJ/FBI, [redacted] and the ultimate decision of

b7E

the President, the NIPC may be may be placed in a direct support role [redacted] or the USIC. See: id., Annex A, p. 12.

B. (U) The Critical Infrastructure Coordination Group is a forum for the convening of Function Coordinators and Sector Coordinators. Where appropriate, the Group is assisted by the Security Policy Board, the Security Policy Forum and the National Security and Telecommunications and Information Systems Security Committee. See: id., Section VI(3).

C. (U) The National Plan Coordination staff serves to integrate the various sector plans into a National Infrastructure Assurance Plan, and to coordinate analyses of the U.S. Government=s own dependencies on critical infrastructures. See: id., Annex A, p. 11. b7E

(U) D. (U) The Terrorist Incident Working group consists of representatives from DOS, Treasury, DOD, DOJ, CIA, JCS, FBI, the Office of the Vice President, the NSC staff and such other departments and agencies as may be necessary. This Group is activated by the Assistant to the President for National Security Affairs, or at the request of any of its members; and it remains convened for the duration of terrorist incidents. See: National Security Decision Directive Number 207, p.3.

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) [redacted]

(U) I. (U) The Counterterrorism Security Group coordinates counterterrorism issues and reviews ongoing crises operations. See: Presidential Decision Directive/NSC-62, p.13.

EFFDATE: 04/29/2002 MCRT# 1262 Div. CY Cav: SecClass: Secret

Section 23-05 (U) Cyber Division - Mission

A. (U) Cyber Division (CyD) is dedicated to applying the highest level of technical capital toward combating cyber-based terrorism, hostile intelligence operations conducted over the Internet, and cybercrime. By aggregating its cyber-centered investigations within one division, the FBI is able to more effectively and efficiently identify, investigate, and neutralize cyber threats. As the nation's cyber dependency becomes even more profound, the Cyber Division will continue to be the vanguard of security for its citizens and its critical infrastructures.

B. (U) The CyD, Computer Intrusion Section (CIS) is charged with providing administrative and operational support and guidance for computer intrusion investigations, including Threats to the

National Information Infrastructure - Counterterrorism / Counterintelligence (TNII-CT/CI) matters and criminal matters. Additionally, CIS coordinates computer intrusion investigations by various criminal investigative and intelligence components of the Federal Government.

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: SecClass: Unclassified

Section 23-06 (U) TNII Matters - Investigative Guidance

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-07 (U) The 288 Subclassification

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-08 288A - Computer Intrusion - Criminal

A. (U) The 288A Subclassification should be utilized upon the receipt of a computer intrusion report and the initiation of a criminal investigation. Examples of criminal computer intrusions include Denial of Service attacks, network intrusions resulting in theft of proprietary or customer information, computer virus attacks which disrupt or destroy data contained on computers, and insertion of malicious computer code which impedes or impairs computer data.
B. (U) As stated in the Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations, "All investigations of crime or crime-related activities shall be undertaken in accordance with one or more of these guidelines." In short, criminal investigative authorities, as set forth in these guidelines, are utilized during investigations of criminal activity, suspected criminal activity, in violation of federal criminal statutes, i.e. the United States Code.
C. (U) Guidance regarding the conduct and reporting of 288A matters can be found in the Manual of Investigative and Operational Guidelines (MIOG), Part 1, Section 288.

EFFDATE: 01/17/2003 MCRT# 1273 Div. CY Cav: SecClass: Unclassified

Section 23-09 (U) 288B - Threats to the National Information Infrastructure - Counterintelligence

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-10 (U) 288C-H - Technical Assistance Matters

A. The 288C-H classifications involve Computer Intrusion Squad technical expert assistance to other program's computer-facilitated crime. Computer Intrusion Squad members should [redacted] noncomputer intrusion matters as follows: b7E
288C Technical Assistance to WCC Program
288D Technical Assistance to VCMO Program
288E Technical Assistance to OC/DP
288F Technical Assistance to CI
288G Technical Assistance to DT Program
288H Technical Assistance to CR Program
288L Technical Support to IT Program

(U) Section 23-11 (S) National HUMINT Collection Directive (NHCD) - The 288I Classification

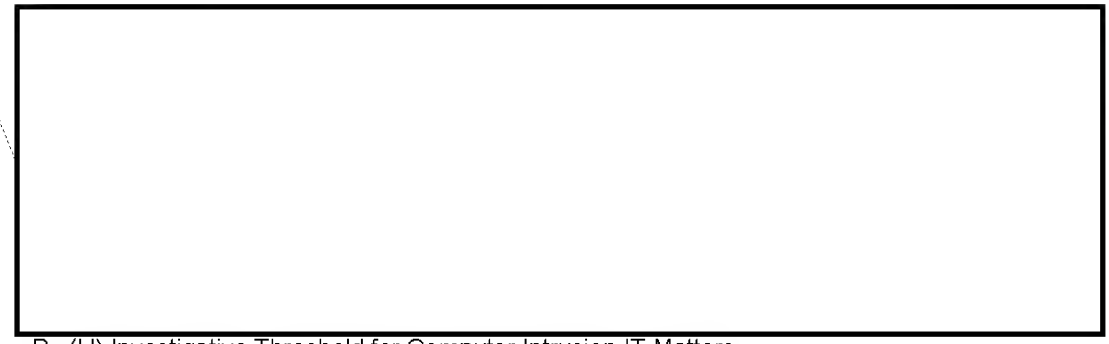
Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 23-12 (U) 288J - Computer Intrusions -International Terrorism (IT) Matters

A. General
1. (U) Computer Intrusions IT investigations are national security investigations in support of the FBI's priority to protect the United States from terrorist attack with the goal of preventing, disrupting, and defeating terrorist operations before they occur. Computer Intrusion IT investigations may often involve, but are not limited to, investigations of person, groups or organizations, who are or may be engaged in activities targeting the national information infrastructure for, on behalf of, or in coordination with a foreign power, or in activities of international terrorism. The purpose of these investigations is to collect information and engage in activities to detect and counteract foreign power sponsored or coordinated international terrorism threats, and clandestine or illegal activities directed against the national security of the United States.
(U) 2. (~~S//NF~~) Pursuant to Part I.A.1. of the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), the Attorney General has authorized the FBI to conduct investigations to obtain information concerning or to protect against threats to national security, including investigations of crimes involved in or related to the national security, as provided in Part II and V of the NSIG, to include international terrorism and foreign computer intrusions Does part ii and V state this verbatim?.
a. Field offices should aggressively pursue Computer Intrusion IT investigations and should develop proactive operations consistent with the NSIG and in consultation with the Cyber Division (CyD). The CyD, in coordination with the Office of Intelligence and Policy Review (OIPR), Department of Justice, is fully engaged to support FBI counterterrorism investigations.
(U) 3. (~~S//NF~~) The CyD will coordinate with the Counterterrorism Division (CTD), as appropriate, at a program level. Field Office Cyber or Computer Intrusion squads should coordinate Computer Intrusion IT investigations with the appropriate CTD squad at the field level.

(S)



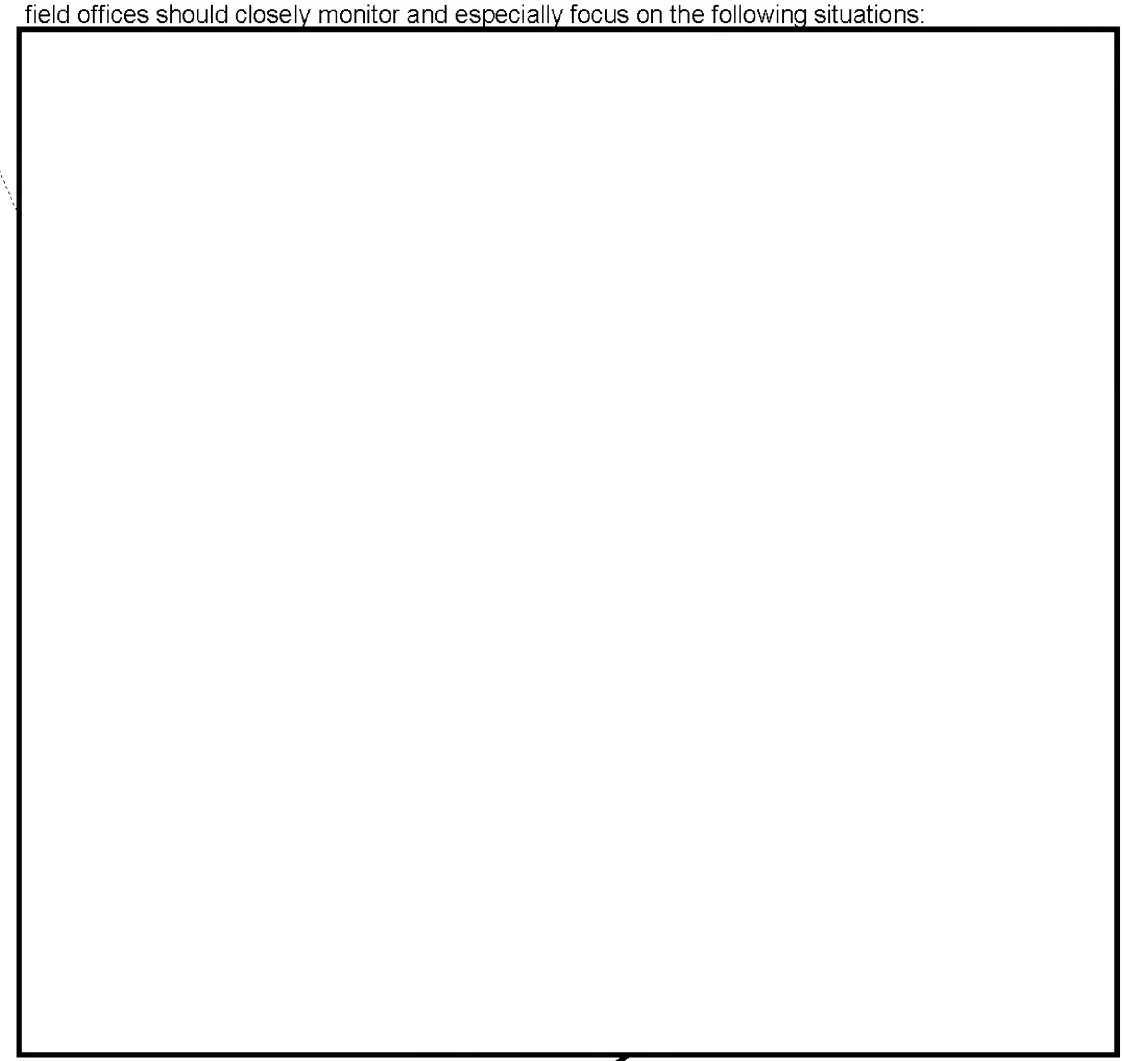
b1

B. (U) Investigative Threshold for Computer Intrusion IT Matters

1. (U) The Computer Fraud and Abuse Act, as amended (the National Information Infrastructure Protection Act of 1996), is the principal federal statute that predicates computer intrusion investigations. The amended statute addresses the central tenets of computer and information system security, i.e., protecting the confidentiality, integrity, and availability of data and systems.

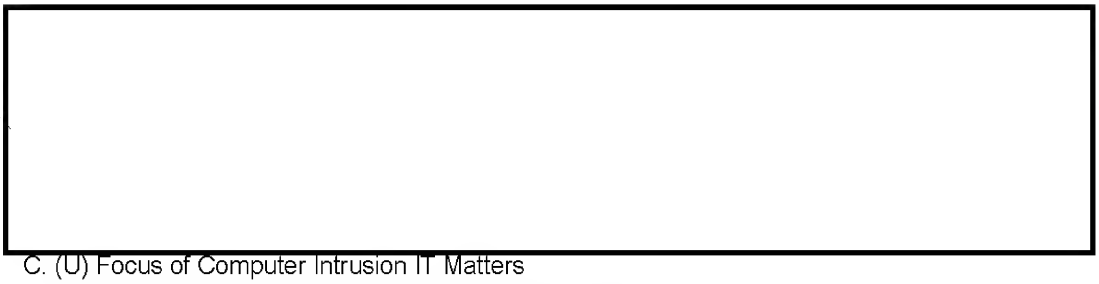
2. (U) Any investigation involving this violation could have national level consequences. However, field offices should closely monitor and especially focus on the following situations:

(S)



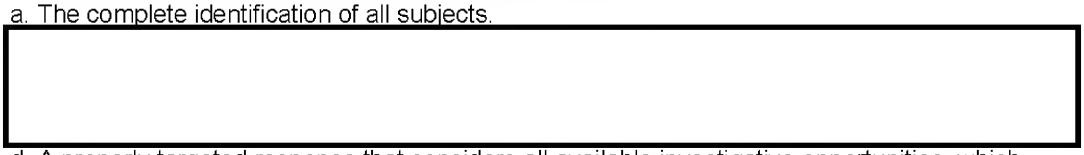
b1
b7E

(S)



b1

C. (U) Focus of Computer Intrusion IT Matters
1. (U) Computer Intrusion IT investigations must focus on:
a. The complete identification of all subjects.



b7E

d. A properly targeted response that considers all available investigative opportunities, which includes criminal prosecution. Because of the potential for eventual criminal prosecution, Computer Intrusion IT investigations should be conducted in a manner that preserves this option whenever possible.
D. (U) Significant Legal Matters
1. (U) Significant legal developments after September 11, 2001 important to Computer Intrusion IT investigations that affected IT investigations include:
(U) a. ~~(S)~~ The Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection, effective October 31, 2003.
b. "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001" (USA PATRIOT Act), effective October 26, 2001; USA Patriot Improvement and Reauthorization Act of 2005; USA Patriot Act Additional Reauthorizing Amendments Act of 2006.
c. "Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI," issued on March 6, 2002 by the Department of Justice (DOJ).
d. Foreign Intelligence Surveillance Court of Review's opinion issued on November 18, 2002, In re Sealed Case, 310 F.3d 717 (FISCR 2002).

Section 23-13 (U) 288J - Authorities, Procedures, and Requirements in Computer Intrusion IT Matters

A. (U) Computer Intrusion IT investigative Authorities and Standards
1. (U) The FBI shall conduct its Computer Intrusion IT investigations in compliance with the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection (NSIG), which were issued October 31, 2003. The general objective of the NSIG is the full utilization of all authorities and investigative techniques, consistent with the Constitution and laws of the United States, so as to protect the United States and its people from terrorism and other threats to the national security.
2. (U) In addition to the NSIG, the FBI shall conduct its Computer Intrusion IT investigations in compliance with the Constitution and all applicable statutes, executive orders, DOJ regulations and policies, and other Attorney General guidelines.
3. (U) FBI Headquarters will be the national program manager and office of origin for all Foreign Terrorist Organizations designated by the U.S. Secretary of State. Field offices direct investigations on the activities of these organizations only within their respective areas of responsibility.

B. Procedural Requirements in Computer Intrusion IT matters

1. (U) There are three levels of investigative activity outlined in the NSIG for the conduct of IT investigations: Threat Assessments, Preliminary Investigations, and Full Investigations.

2. (U) A Computer Intrusion IT investigation in the 288J classification must be initiated when investigative steps are taken by the investigative personnel involved in either a Preliminary or Full investigation.

a. All investigative cases on individuals, groups, or organizations in the 288J classification must be characterized as either a Preliminary or Full Investigation. Control files are not investigative cases and thus are not designated as either a Preliminary or Full Investigation. b7E

b. Preliminary and Full Investigations of groups and organizations should focus on activities related to threats to the national security, not on unrelated First Amendment activities. Any information concerning a group or organization that is relevant to the investigation of a threat to the national security may be sought, including information on

(U) X

(S)

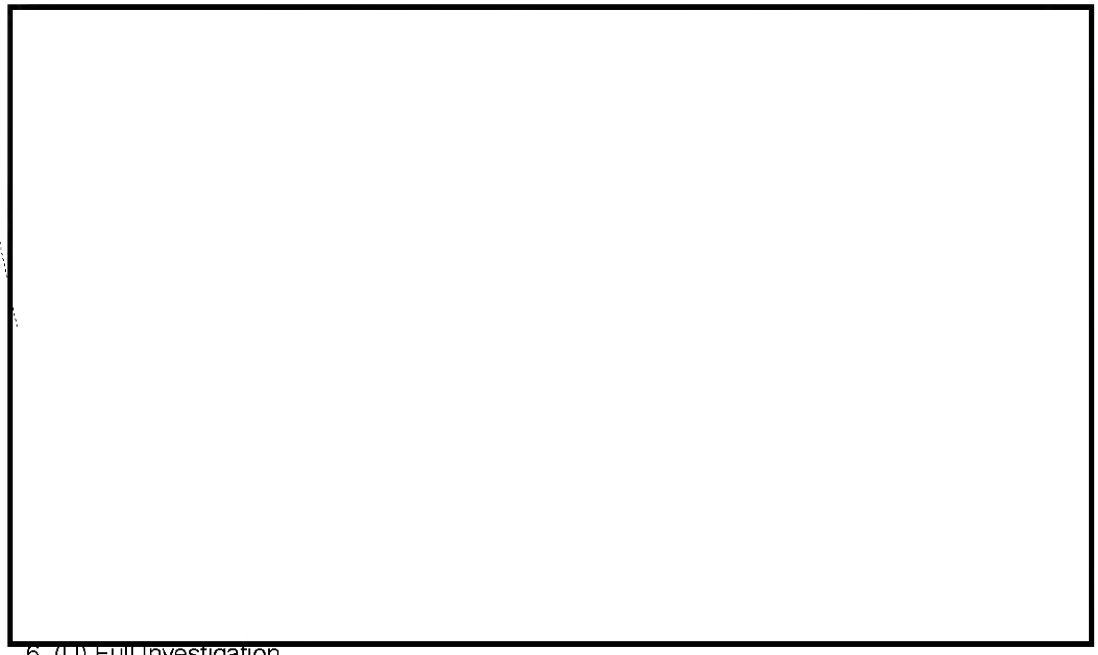
b1

(S) [redacted] b1

(U) (1) (S) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

(S) [redacted] b1

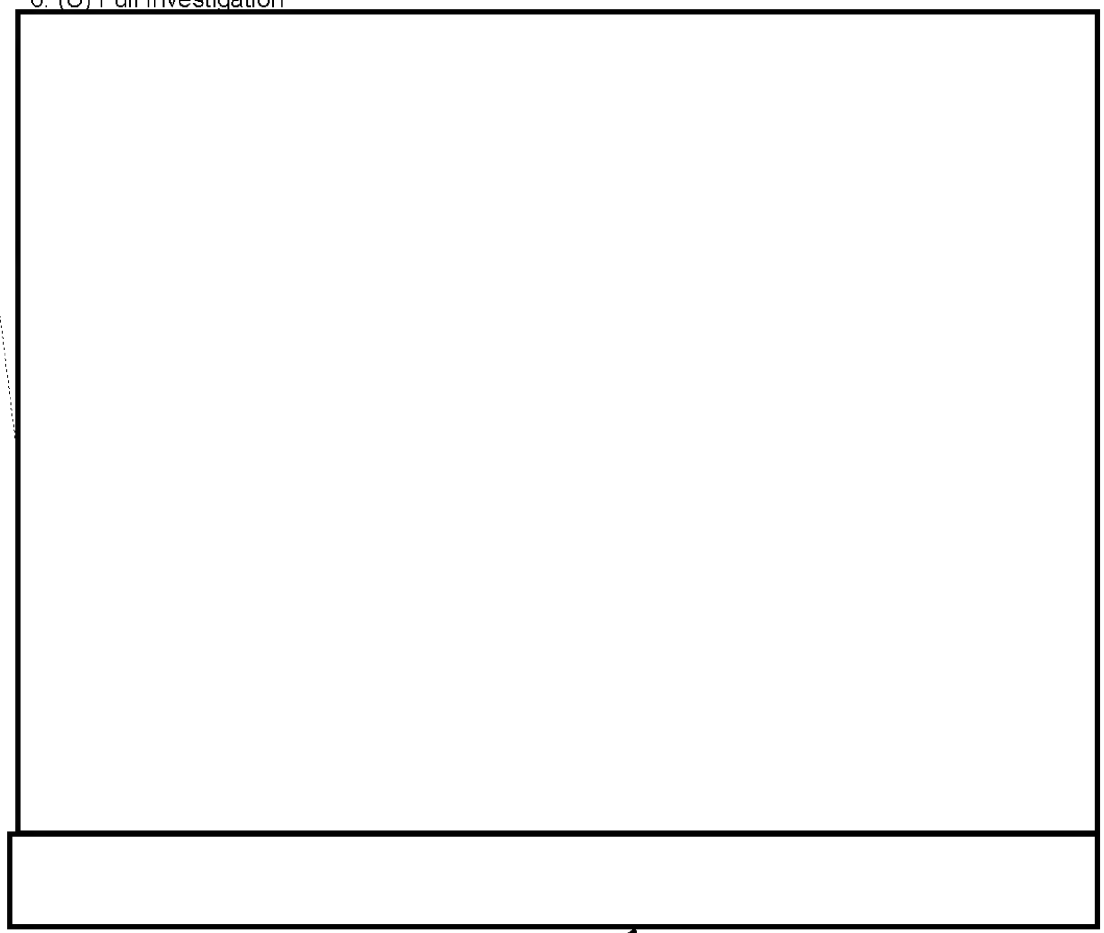
(S)



b1

6. (U) Full Investigation

(S)



b1

b1
Referral/Consult

(S) [redacted]

(U) (1) (S) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

(S) [redacted] b1

(U) h. (S/NF) The Office of Origin is determined by the residence, location or destination of the subject of the investigation. If special circumstances exist, for example, [redacted] b7E origin may be assumed by the office having the most compelling investigative interest. Uncertainties regarding the appropriate Office of Origin shall be resolved by FBIHQ.

(S) [redacted] b1

(U) 5. (~~S~~) A sensitive national security matter is defined in the NSIG as: "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials." b7E

(U) [redacted]

D. (U) Notification of Case Opening

(S) [redacted] b1

(S) [redacted] b1

F. (U) United States Person

1. (U) A United States Person is defined in the NSIG as one of the following:

a. an individual who is a United States citizen or an alien lawfully admitted for permanent residence;

b. an unincorporated association substantially composed of individuals who are United States person; or

c. a corporation incorporated in the United States.

2. (U) In the absence of information establishing otherwise, subjects are presumed to be U.S. Persons.

3. (U) A foreign power as defined in Part VIII.L.1.-3. of the NSIG is never to be considered a United States person, including any foreign government or component thereof, any faction of a foreign nation or nations not substantially composed of individuals who are United States persons, or any entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

G. (U [redacted]

1. (U) The notification requirements to CyD of the initiation of a new computer intrusion IT investigation, described above, do not obviate the need or negate the requirement to submit [redacted] b7E

H. Undercover Operations in Computer Intrusion IT matters

(U) 1. ~~(S//NF)~~ The use of undercover operations as an investigative technique in Computer Intrusion IT matters can be very productive. However, inherent in the use of such techniques are legal, operational and policy considerations. Guidelines set forth in Section 28, infra, of this manual are applicable to all Computer Intrusion IT undercover operations and should be utilized to efficiently establish and manage undercover operations.

I. Extraterritorial operations in Computer Intrusion IT matters

[redacted]

J. (U) Computer Intrusion IT matters and Criminal Programs
1. (U) An computer intrusion IT investigation might also impact criminal programs overseen by the Criminal Investigative Division (CID). In those instances, the appropriate CID unit should also be apprised of the investigation in the initial communication to CyD.
2. (U) Any investigation properly opened as an International Terrorism investigation after delineating specific facts clearly establishing a terrorism nexus, which also possesses a drug nexus, must be conducted not only in conformance with the NSIG, but also in accordance with existing guidelines as stated in MIOG, Part 1, Sections 245 and 281. Since the need for interagency coordination is particularly acute with regard to drug matters, the initial communication advising CyD of the computer intrusion IT case initiation must also be directed to the CID, Drug Section. If there is an international nexus, then a copy should also be directed to the appropriate Legal Attache for information.
K. (U) Case Title Examples

(S) [redacted] b1

4. (U) File numbers are unclassified. Case titles, except code word titles, are classified.

[redacted] b7E

[redacted] b7E

M. (U) Unaddressed Work
1. (U) There will be no unaddressed work within the Computer Intrusion IT program of any field office.
N. (U) Code Word Operations
1. (U) As appropriate, code word operations may be opened as Computer Intrusion IT investigations and conducted in accordance with a Preliminary Investigation or Full Investigation.
O. (U) Control and Administrative Files (See MAOP, Part 2, 2-4.1.2 and 2-4.1.5)
1. (U) Control files in the 288J classification (288J-FO-C) may be maintained by field offices. Control files are separate files established for the purpose of administering specific phases of an investigative matter or program and would not be considered a PI or FI. They are neither Preliminary nor Full Investigations and thus do not require [redacted]
2. (U) The 288J zero (288J-0) file may be utilized for material which does not require investigation, such as complaints that have been addressed, but were deemed not credible. Investigative leads cannot be set out of the 288J zero file.
P. (U) Sub-File Folders
1. (U) Routine Folders should be opened within the Computer Intrusion IT investigation in accordance with the standards outlined in MAOP, Part 2, 2-5.1. The list of approved folders includes:
1A 1A Section exhibits1B FD-192s (evidentiary bulkies)
1C FD-192s (nonevidence bulkies)
BC Background Information
CE Case Expenditures
ELA ELSUR Administrative
ELA1 ELSUR Original Logs
ELA1A ELSUR Copies and Logs
ELA1B ELSUR Transcripts
GJ Grand Jury Material
FISUR Physical Surveillance Logs
FF Forfeiture Matters
LAB Laboratory/Latent Reports
MC Mail Cover Materials
NC Newspaper Clippings (Press Releases)
SBP Subpoenas
TEL Telephone Subscriber and Toll Information
2. (U) In addition, Special Category Folders should be opened to organize specific investigative aspects of the case file. These folders should be created when information pertinent to the categories arises in the case. These special categories include:
a. FOREIGN Foreign Intelligence--for which permission would need to be granted from a host government prior to release to a third party (for example, the U.S. Attorney's Office).
b. OGA Intelligence from other government agencies--for which permission to disseminate would be required from the originating service (for example, the Naval Criminal Investigative Service).
c. TERRFIN Terrorist Financing--for information related to the funding of terrorism.
d. CRIMINAL For evidence and other information regarding investigation being pursued relating to specific acts of criminality.

(U) Q. (U) Approval Authority for Interviews in Computer Intrusion IT Investigations b1

(S) [redacted]

(S) [redacted] b1

R. (U) Classification

1. (U) It is important that investigators NOT overly classify information in terrorism investigations. Classification derives from the source of and method used to obtain the information, not the actual content of the information.

(U) [redacted] b7E

4. (U) Situations will often arise when classified information obtained during a Computer Intrusion IT investigation will be relevant to a criminal or civil proceeding. In this instance, a declassification review will be required, which, in turn, often requires a more fulsome translation effort than has been previously undertaken. FBI field offices must ensure the declassification review process is coordinated with the National Security Law Branch, Office of the General Counsel, and relevant CyD substantive units. If information was properly classified when placed in the case file, the review process will be much more efficient. If the litigation is a criminal case, further coordination may be required with the Department of Justice Criminal Division and relevant United States Attorney's Offices. Any information that should remain classified, and which is relevant to a criminal proceeding, will be managed under the Classified Information Procedures Act (CIPA). Classified information relevant to a civil proceeding may require a claim of State Secrets, which will require substantial involvement with the Civil Division of the Department of Justice and the personal intervention of the Attorney General (or other relevant Cabinet Officer).

S. (U) The Foreign Intelligence Surveillance Court (FISC)

(S) [redacted] b1

T. (U) Attorney-Client Privilege

(S) [redacted]

(S) [redacted] b1

U. (U) Violent Gang and Terrorist Organization File (VGTOF) and Terrorist Screening Center (TSC) Database

1. (U) Subjects of both Preliminary and Full Investigations must be entered into the Violent Gang and Terrorist Organization File (VGTOF) by completing an FD-930. In the FD-930, case Agents must make a recommendation [redacted] as to which databases the subject should be entered and a recommended Handling Code. Upon closing the Preliminary or Full Investigation, the case Agent shall remove subjects who no longer merit inclusion via form FD-930. b7E

2. (U) The "Miscellaneous" field on the FD-930 should include the case Agent's name and 24/7 contact number, the subject's USPER status and country of citizenship, and any other pertinent information. CLASSIFIED INFORMATION MAY NOT BE LISTED IN THE "MISCELLANEOUS" FIELD.

3. (U) The databases into which a subject can be entered will be listed in the FD-930, but they include the Violent Gang and Terrorist Organization File (VGTOF), TSA No Fly or TSA Selectee lists, Treasury Enforcement Communications Systems (TECS), and Consular Lookout and Support System (CLASS) for non-USPERs.

4. (U) The Handling Codes categories, and a description of each, will be listed in the FD-930.

V. (U) Information Sharing

1. (U) Information acquired during the course of a Computer Intrusion IT investigation should be shared as consistently and fully as possible among agencies with relevant responsibilities to protect the United States and its people from terrorism and other threats to national security, except as limited by specific statutory or policy constraints. Information may be disseminated to obtain information for the conduct of a lawful investigation by the FBI.

2. (U) The FBI (through CyD) shall keep the DOJ Criminal Division and the Office of Intelligence Policy and Review apprised of all information obtained through the conduct of Computer Intrusion investigations, except as limited by orders issued by the FISC, controls imposed by the originators of sensitive material, or restrictions established by the Attorney General or the Deputy Attorney General in particular cases.

3. (U) Subject to the conditions and terms described in the NSIG, relevant United States Attorney's Offices (USAOs) shall receive information and engage in consultations to the same extent as allowed the DOJ Criminal Division. Thus, the USAOs shall have access to information, shall be kept apprised of information necessary to protect national security and information concerning crimes, shall receive notices of the initiation of investigations and annual summaries, and shall have access to FBI files, to the same extent as the DOJ Criminal Division.

4. (U) Information disseminated to a USAO shall be disseminated only to the United States Attorney (USA) and/or any Assistant United States Attorneys (AUSAs) designated to the DOJ by the USA as points of contact to receive such information. The USA and AUSAs shall have appropriate security clearances and shall receive training in the handling of classified information and information derived from FISA, including training concerning restrictions on the use and dissemination of such information. A disseminable LHM is the appropriate method for presenting investigative findings to the Department of Justice. A copy of the LHM must also be directed to the appropriate CyD operational unit.

5. (U) Pursuant to the Attorney General's Intelligence Sharing Procedures, dated March 6, 2002, the FBI must keep a designated AUSA in the relevant USAO fully informed of all relevant foreign intelligence information, as well as evidence of any crime, including information and evidence obtained or derived from FISA, which arises during International Terrorism investigations. Information obtained or derived from FISA shall be marked as required in Title 50, United States Code, Sections 1806(b) and 1825(c).

6. (U) Foreign intelligence is defined in the NSIG as: "information relating to the capabilities, intentions, or activities of foreign powers, organizations, persons, or international terrorist activities."

W. Investigative Accomplishments (FD-542) in Computer Intrusion IT Matters

1. The FD-542 shall be utilized to capture statistical accomplishments not already captured in [redacted] which utilizes the FD-515 to capture data relative to traditional criminal statistical accomplishments. Although the method of capturing statistical accomplishments through the FD-515 [redacted] should be used when appropriate, the FD-542, through the FD-542 macro, shall be utilized to capture investigative accomplishment identified in Section 2-53, supra, relevant to national security and international terrorism investigations. b7E

X. Closing Computer Intrusion IT Matters

1. General

a. Prior to closing a Computer Intrusion IT investigation in the 288J classification, Field offices must ensure all reasonable investigative techniques have been exploited. By closing the investigation, the field office is affirming it has exhausted all reasonable and practical intelligence collection methods with respect to the investigation.

b. If the investigation has uncovered criminal violations of state or federal law, then a declination from the United States Attorney's Office must be received and documented within the investigative case file.

2. Closing Communication to FBIHQ

a. The closing communication will be sent to the CIS, CyD to the attention of the following:

(1) CyD Substantive section/unit

(2) CTD Substantive section/unit

(3) [redacted] b7E

(4) CT Analytical Section

(5) [redacted]

(6) Other sections or units, as appropriate

(7) Appropriate field office or Legal Attaché ("Legat"), if subject relocated

b. An FD-930 will be enclosed to remove or modify the entry in VGTOF.

c. The Details section of the closing communication will contain the following information:

(1) The type of investigation (i.e., Preliminary or Full)

(2) The date it was opened

(3) The date it was converted from a Preliminary Investigation to Full Investigation, if applicable

(4) If a Full Investigation, then the date and serial number of the most recent Annual Summary

(5) Whether the investigation involves a United States person

(6) An assessment of the extent to which the subject is (or members of the group are) aware of the terrorist aims of the foreign power

(7) Any sensitive national security matters, which is defined in the NSIG as "a threat to the national security involving the activities of an official of a foreign country other than a threat country, a domestic public official or political candidate, a religious or political organization or an individual prominent in such an organization, or news media, or any other matter which, in the judgment of the official authorizing an investigation, should be brought to the attention of FBI Headquarters and other Department of Justice officials."

(8) Name and all aliases of the subject and complete biographical information regarding the subject

(9) A summary of the investigation to include a list of the investigative techniques used, to include:

[redacted] b7E

[redacted]

b7E

(10) Whether the case was submitted to the United States Attorney's Office for criminal prosecution and result (indictment or declination); if there is a criminal declination, then the case Agent prepares a letter to the United States Attorney's Office that documents the declination, the letter must be uploaded into the case file, and referenced in the closing communication

3. Reason(s) for Closure of Case

a. Reason(s) for Closure of Case

(1) Subject was convicted

(a) Include details, to include jurisdiction, statute(s), and sentence

(2) Subject is incarcerated

(a) Include details, to include jurisdiction, statute(s), sentence, incarceration facility, projected release date

(b) Incarceration of a subject, by itself, does not meet the basic investigative standard which would merit an international terrorism case to be closed. Factors to be considered prior to closing include, but are not limited to: [redacted]

(4) Subject is believed to have moved out of the field office's area of responsibility, but stayed within the USA

(a) include details, to include travel information, traveled with whom, location to which subject moved, and which field office has jurisdiction

(b) The change of residence of a subject, by itself, does not meet the basic investigative standard which would merit an IT case to be closed. If a subject has moved outside the area of

responsibility of a field office, then the current office of origin will prepare a communication transferring the investigation to the field office covering the subject's new residence. This communication will summarize the investigation to date and include action leads to both the new field office and the appropriate CyD substantive unit(s) to ensure a seamless and fluid transition between the two field offices.
(5) Subject is believed to be deceased
(a) Include details, to include basis for belief and circumstances of death
(6) Allegations against the subject are without merit
(a) Include details
4. (U) Leads
a. It is not possible to set leads, including information-only leads, on closing communications or cases in closed status
Y. Completion and Submission of the FD-930
1. Completion of Gang, Subgroup, and File # fields
a) In the Gang field, enter "International Extremist"
b) In the Subgroup field, enter the VGTOF handling code (1, 2, 3, 4, or silent hit)
c) In the File # field, enter the substantive 288J file number, not an administrative file number (such as the 66 classification) or other control file number
2. To remove or modify a record in VGTOF, send a copy of the closing communication and an enclosed FD-930 to the [redacted] Check the "Remove" box or the "Supplements Initial Submission" box at the top of the form. The FD-930 must be sent directly to the [redacted] not to the substantive unit. b7E
3. All subjects of Preliminary Investigations must be removed from VGTOF and other watch lists when the case is closed.
4. Subjects of Full Investigations may remain in VGTOF and other watch lists, if appropriate. Example: The subject of a Full Investigation is still a threat to national security, but moves to another field office's area of responsibility or outside the USA and thus the field office closes its case. Notify appropriate field office or Legat in the Details area of the closing communication
Z. (U) The Behavioral Analysis Program
1. (U) See: Section 2-35, supra.

Section 23-14 (U) 288L - Technical Support to International Terrorism Matters

A. General
1. (U) Technical Support to International Terrorism investigations are conducted in support of the FBI's priority to protect the United States from terrorist attack with the goal of preventing, disrupting, and defeating terrorist operations before they occur. The purpose of these investigations is to provide expert technical assistance in international terrorism investigations, when the basis for the international terrorism investigation does not warrant opening a Preliminary Inquiry or Full investigation under the 288J classification.
B. Authorities and Requirements in Technical Support to International Terrorism Matters
(U) 1. (S) Authority for conducting the investigative techniques in a 288L Technical Support investigation rests with the squad supervisor. b7E
(U) 2. (S) A 288L technical support investigation may only be opened in support of an authorized [redacted]
(U) 3. (S) Unlike 288J classification reporting requirements for Preliminary Inquiry and Full investigations, a technical support investigation does not have specific reporting requirements.

[redacted]

b7E

(U) 4. (S) Significant Investigative Milestones- major investigative steps shall be provided to FBIHQ by an official communication on a timely basis when they occur, irregardless of other reporting requirements.

(U) 5. (S) Investigations under the 288L classification must be closed before or at the same time as the corresponding international terrorism matter.

Section 23-15 (U) Relevant Statutes

18 U.S.C. § 1030. Fraud and related activity in connection with computers
(a) Whoever--
(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;
(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--
(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);
(B) information from any department or agency of the United States; or
(C) information from any protected computer if the conduct involved an interstate or foreign communication;
(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;
(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;
(5)(A)(i) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;
(ii) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or
(iii) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage; and
(B) by conduct described in clause (i), (ii), or (iii) of subparagraph (A), caused (or, in the case of an attempted offense, would, if completed, have caused)--
(i) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related

course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;
(ii) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;
(iii) physical injury to any person;
(iv) a threat to public health or safety; or
(v) damage affecting a computer system used by or for a government entity in furtherance of the administration of justice, national defense, or national security;
(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--
(A) such trafficking affects interstate or foreign commerce; or
(B) such computer is used by or for the Government of the United States; [FN1]
(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to cause damage to a protected computer; shall be punished as provided in subsection (c) of this section.
(b) Whoever attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.
(c) The punishment for an offense under subsection (a) or (b) of this section is--
(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), (a)(5)(A)(iii), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--
(i) the offense was committed for purposes of commercial advantage or private financial gain;
(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or
(iii) the value of the information obtained exceeds $5,000; and
(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and
(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4) [FN2] (a)(5)(A)(iii), or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;
(4)(A) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 10 years, or both, in the case of an offense under subsection (a)(5)(A)(i), or an attempt to commit an offense punishable under that subsection;

(B) a fine under this title, imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(5)(A)(ii), or an attempt to commit an offense punishable under that subsection;
(C) except as provided in paragraph (5), a fine under this title, imprisonment for not more than 20 years, or both, in the case of an offense under subsection (a)(5)(A)(i) or (a)(5)(A)(ii), or an attempt to commit an offense punishable under either subsection, that occurs after a conviction for another offense under this section; and
(5)(A) if the offender knowingly or recklessly causes or attempts to cause serious bodily injury from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for not more than 20 years, or both; and
(B) if the offender knowingly or recklessly causes or attempts to cause death from conduct in violation of subsection (a)(5)(A)(i), a fine under this title or imprisonment for any term of years or for life, or both.
(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.
(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.
(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.
(e) As used in this section--
(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;
(2) the term "protected computer" means a computer--
(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or
(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;
(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;
(4) the term "financial institution" means--
(A) an institution, [FN3] with deposits insured by the Federal Deposit Insurance Corporation;
(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;
(C) a credit union with accounts insured by the National Credit Union Administration;
(D) a member of the Federal home loan bank system and any home loan bank;
(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;
(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;
(G) the Securities Investor Protection Corporation;
(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and
(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;
(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;
(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;
(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;
(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;
(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;
(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and
(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.
(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.
(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in clause (i), (ii), (iii), (iv), or (v) of subsection (a)(5)(B). Damages for a violation involving only conduct described in subsection (a)(5)(B)(i) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.
(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5). 18 U.S.C. § 2703. Required disclosure of customer communications or records
(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.
(b) Contents of wire or electronic communications in a remote computing service.--(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or
(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--
(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or
(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.
(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--
(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and
(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.
(c) Records concerning electronic communication service or remote computing service.--(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--
(A) obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant;
(B) obtains a court order for such disclosure under subsection (d) of this section;
(C) has the consent of the subscriber or customer to such disclosure;
(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or
(E) seeks information under paragraph (2).
(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--
(A) name;
(B) address;
(C) local and long distance telephone connection records, or records of session times and durations;
(D) length of service (including start date) and types of service utilized;
(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and
(F) means and source of payment for such service (including any credit card or bank account number), of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).
(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.
(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. In the case of

a State governmental authority, such a court order shall not issue if prohibited by the law of such State. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify such order, if the information or records requested are unusually voluminous in nature or compliance with such order otherwise would cause an undue burden on such provider.

(e) No cause of action against a provider disclosing information under this chapter.--No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter.

(f) Requirement to preserve evidence.--

(1) In general.--A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

(2) Period of retention.--Records referred to in paragraph (1) shall be retained for a period of 90 days, which shall be extended for an additional 90- day period upon a renewed request by the governmental entity.

(g) Presence of officer not required.--Notwithstanding section 3105 of this title, the presence of an officer shall not be required for service or execution of a search warrant issued in accordance with this chapter requiring disclosure by a provider of electronic communications service or remote computing service of the contents of communications or records or other information pertaining to a subscriber to or customer of such service.

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 5
Page 6 ~ b1, b7E
Page 7 ~ b1
Page 11 ~ b1
Page 15 ~ b1
Page 19 ~ b1, b7E, Referral/Consult

Section 24 (U) Targeting the U.S. Government Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Section 25 (U) Perception Management Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

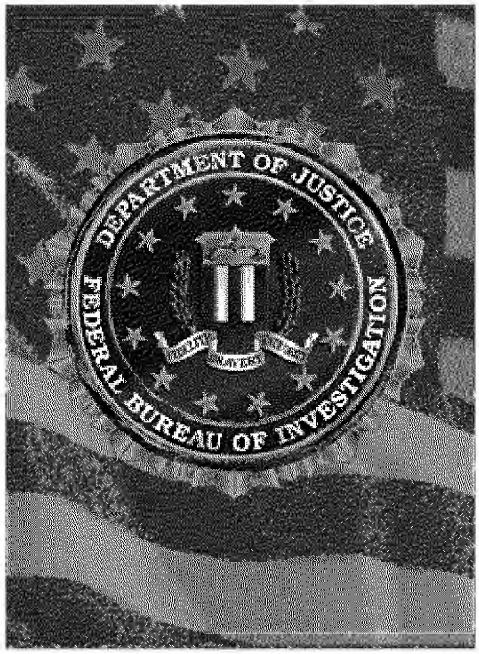
Section 26 (U) Foreign Intelligence Activities Investigations

Section 26-01 (U) Foreign Intelligence Activities Investigations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Eff. Date: 08/09/2010

Confidential Human Source Policy Manual



Federal Bureau of Investigation (FBI)

POL07-0004-DI

Revised September 5, 2007

GENERAL INFORMATION: Questions or comments pertaining to this handbook can be directed to:

b6
b7C
b7E

FBIHQ/[redacted] Unit Chief [redacted]

FBIHQ/Directorate of Intelligence, Division 19, National Security Branch

(NOTE: This document supersedes the Manual of Investigative Operations and Guidelines [MIOG] [redacted] and the National Foreign Intelligence Program Manual [NFIPM], Section 27).

b7D

PRIVILEGED INFORMATION:

Any use of this report, including direct quotes or identifiable paraphrasing, will be marked with the following statement:

This is a privileged document that cannot be released in whole or in part to persons or agencies outside the Federal Bureau of Investigation, nor can it be republished in whole or in part in any written form not containing this statement, including general use pamphlets, without the approval of the Director of the Federal Bureau of Investigation.

FOR OFFICIAL FBI INTERNAL USE ONLY—DO NOT DISSEMINATE

~~SECRET//NOFORN~~

CLASSIFIED BY: Multiple Sources

DECLASSIFY ON: ~~4/17/2032~~

Table of Contents

b7E

b7E

b7E

b1
b7E

b7E

List of Appendices

b1
b7E

1. Scope

Purpose: (U//FOUO) To provide comprehensive policy regarding Confidential Human Sources (CHS).

Background: (U//FOUO) Under the authority of the new Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources (AGGs CHS), the Directorate of Intelligence (DI) [redacted] created this Manual, so the Federal Bureau of Investigation (FBI) can meet its mission of intelligence collection in order to respond to investigative program priorities and to national level and FBI intelligence collection requirements. Furthermore, this Manual comprehensively addresses all CHS administration. b7E

(U//FOUO) This Manual was validated and approved by all relevant substantive divisions and the Office of General Counsel.

Intended Audience: (U//FOUO) This Manual is intended for all FBI personnel who have a role in the administration of CHSs.

1.1. Overall Program Directives

1.1.1. Responsibility for the Development and Operation of Confidential Human Sources

(U//FOUO) The FBI operates CHSs to meet its mission of intelligence collection in order to respond to investigative program priorities and to national level and FBI intelligence collection requirements. [redacted] b7E

[redacted] Therefore, the Assistant Director in Charge (ADIC) or Special Agent in Charge (SAC) of each Field Office[1] (FO) in the FBI is responsible for ensuring that the FO has a viable CHS Program that contributes to the FBI's collective Human Intelligence (HUMINT) base. ADICs, SACs, and members of the FO's Investigative and Intelligence Operations management staff, to include Assistant Special Agents in Charge (ASAC) and Supervisory Special Agents (SSA), are to ensure that the FO fulfills its intelligence collection and information dissemination mission in compliance with FBI's protocols, rules, and regulations, including those contained in this Confidential Human Source Policy Manual (CHSPM). SACs shall implement a comprehensive periodic training of respective personnel regarding the AGGs CHS and CHS policy.

(U) It is a core responsibility of each Special Agent (SA) to develop and maintain a CHS base from which to collect vital information on FBI investigative and national intelligence priorities. [redacted] b7E

[1](U) This Manual refers to all FBI Field Offices and Field Divisions as FO in order to distinguish them from FBIHQ components.

b7E

[redacted]

(U//FOUO) No member of the FBI's management staff or non-Agent personnel shall be the Case Agent (CA) for the operation of a CHS. Only FBI SAs shall serve as CAs whereas SSAs and other management staff are responsible for the oversight and management of the CHS program. SAs serving as Co-CAs have all the same duties and responsibilities as CAs. Legal Attaches (Legat) and Assistant Legat Attaches (ALAT) are allowed to operate CHSs when circumstances dictate. CHS management responsibilities may not be delegated to non-Agent personnel.

1.2. Use of the Confidential Human Source Program

(U) Use of the CHS program is warranted when it is prudent and necessary to provide protection to (a) the identity of the CHS of needed information, (b) the information itself, or (c) the CHS's relationship with the FBI. For purposes of this Manual, a CHS is any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional, useful, and credible information in the future and whose identity, information, or relationship with the FBI warrants confidential handling.

(U) In general, an individual should not be opened as a CHS [redacted] when there is no logical reason for confidentiality or when the individual holds a position that would normally compel him/her to provide the information, such as a U.S. law enforcement officer or a U.S. public official. Exceptions would include instances [redacted]

b7E

(U) Nothing in this policy manual is intended to create or does create an enforceable legal right or private right of action by a CHS or any other person.

1.3. Automated System Entry of Confidential Human Source Files

(U) All communications must be entered into the FBI's automated case management system. [redacted]

b7E

1.4. Sharing of Intelligence

(U) CHS information that has intelligence value should be shared with other squads, FOs, FBI Headquarters (FBIHQ), [redacted] (See Section 2, FBI's General Policy for Intelligence Dissemination of the FBI's Intelligence Policy Manual.) [redacted] Dissemination is the responsibility of the [redacted] or the appropriate substantive units at FBIHQ.

b7E

(U) When an FBI FO determines that information from any CHS affects investigative matters in another FBI FO, then that information must be forwarded to the other FO

under the substantive case caption (see Section 15, Dissemination and Disclosure of the Confidential Human Source's Identity).

1.5. Classified Information

(U) If the CHS's background information or the information reported reflects matters of national security requiring classification, that information must be appropriately classified based on an assessment of the harm to national security that its unauthorized disclosure would cause. [redacted] b7E [redacted] (See Section 16.2, Files) (See the DI Security Classification Guide for additional guidance.)

1.6. Principles of Confidentiality

(U) Protection of the true identity of any CHS is always the primary concern in any decision related to disclosure. This principle extends even to decisions to disseminate the identity within the Department of Justice (DOJ) and among task force partners. SAC approval may be required for disclosure of a CHS's identity or information that the CHS has provided which would have the tendency to identify the CHS as designated in this manual. An FBI employee's obligation to maintain the identity of and information from or regarding any CHS as confidential continues after leaving his/her employment with the FBI. FBI Agents may advise CHSs that a CHS's disclosure of his/her relationship with the FBI may jeopardize the relationship and its effectiveness.

1.7. Confidential Human Source Coordinator (CHSC)

(U) Each FO has at least one SA and one alternate SA who serve(s) as the FO's full-time Confidential Human Source Coordinator (CHSC), and who would be assigned to the FO's FIG SSA or the ASAC for intelligence matters. It is at the discretion of the SAC/ADIC whether additional personnel would be assigned to these duties.

(U) CHSCs are responsible for the oversight and compliance matters of the FO's CHS program. (See Field Office Intelligence Handbook, Annex 3: Human Source Coordination.) However, ultimate responsibility for CHS management must lie with FBI supervisors who are in a position of authority over the management of the CHS.

(U) Independently, the AGGs CHS mandate that DOJ appoint a CHSC who is a supervisory Federal Prosecuting Office[2] (FPO) Attorney[3] designated by each Chief

[2](U) Federal Prosecuting Offices include the following DOJ components: United States Attorney Offices, the Criminal Division, the National Security Division, or any other litigating component of the Department of Justice with authority to prosecute federal criminal offenses, including the relevant sections of the Antitrust Division, Civil Division, Civil Rights Division, Environmental and Natural Resources Division, and the Tax Division.

[3](U) FPO Attorney is an attorney employed by or working under the direction of an FPO.

Federal Prosecutor[4] (CFP) to facilitate compliance with the AGGs. This Manual refers to these individuals as DOJ's CHSC.

1.8. [redacted] b7E

[redacted]

1.9. Conveying Information to the Confidential Human Source

(U) [redacted]

1.10. Approvals, Authorities, and Delegation

(U) Unless specified otherwise in this manual (i.e., may not delegate), all approval authorities may be delegated to any FBI Agent in a supervisory position. Approval authorities may be provided by anyone in an acting capacity or a higher ranking position than that required.

1.11. Audio and Video Recording

(U//FOUO) [redacted] b7E

1.12. Prohibitions

(U//FOUO) At all times when interacting with a CHS, an FBI employee must conduct himself/herself professionally according to FBI standards and instructions regarding FBI employee conduct. (See Manual of Administrative Operations and Procedures [MAOP], Part I, Section I-1 and The Employee Handbook, Page 26 of 11/2003 edition.)

(U//FOUO) FBI Agents shall not be opened as CHSs.

(U//FOUO) FBI personnel directing, overseeing the direction of, or closely involved with the operation of a CHS may never:

- [redacted] b7E

[4](U) A CFP is the head of a Federal Prosecuting Office.

- Interfere with, inappropriately influence, or impede any criminal investigation, arrest, or prosecution of that CHS or any civil action in which the CHS is a litigant or witness
- [redacted] b7E
- Provide to or receive from the CHS anything of more than nominal value (See Section 1.13., Exceptions.)
- [redacted] b7E
- [redacted]
- Authorize a CHS to participate in an act of violence, [redacted]
- [redacted] b7E
- [redacted]
- [redacted] to a CHS unless necessary for CHS operations
- [redacted]
- Socialize with the CHS, except to the extent necessary and appropriate for operational reasons. Meals with CHSs for rapport building and conducting business are considered appropriate. (See Section 1.13., Exceptions.)
- [redacted] b7E

[redacted] b7E
authorized to do so by the CFP or his/her designee and after consulting with the SAC. [redacted]

1.13. Exceptions

(U//FOUO) [redacted] b7E

(U//FOUO) If an FPO is participating in the conduct of an investigation or prosecution[5] utilizing the CHS, the FBI shall provide written notice (with a copy to the CHS file) to the FPO Attorney, in advance whenever possible, if the FBI approves such an exception or if an FBI Agent socializes with the CHS in a manner not permitted.

1.14. Removing CJIS Division/NCIC "Stop Notices"

(U/FOUO) [redacted] b7E

[redacted] Stop notices are removed by CJIS, upon notification by [redacted] when the CHSs are closed.

[5](U) Any FPO employing or directing an FPO Attorney assigned to a matter whose approval is necessary pursuant to the AGGs CHS, or whose approval was sought or obtained regarding any investigative or prosecutorial matter including the issuance of a search or arrest warrant, electronic surveillance order, subpoena, indictment, or other related matter.

2. Opening a Confidential Human Source

2.1. Opening Communication

(U) As part of the [redacted] the CA must prepare an opening communication approved by an SSA with notification to [redacted] for information. Upon receipt, [redacted] conducts a universal query to determine whether the CHS has been opened in another FO. FOs are expected to conduct local queries and more comprehensive searches, if readily available. b7E

(U) In addition to other requirements, which must be addressed when opening (see Section 4, Instructions To Be Discussed with a Confidential Human Source, Section 5, Special Approval Requirements, and Section 6, [redacted] the following information must be documented in the CHS's file:

- [redacted]
- b7E

- (U) Investigative classification(s)/type of information on which the CHS reports
- (U) If known, subject or group on whom the CHS reports.
- [redacted] b7E
- (U) CA and Co-CA's name, and state whether FBI, Task Force Officer (TFO), [redacted] b7E
- (U) FO and squad handling the CHS
- (U) [redacted] b1 b7E
- (S) [redacted]
- (U) [redacted] b7E
- (U) [redacted]
- (U) [redacted] b7E
- (U) [redacted]
- (U) [redacted]

(U//FOUO) Whether special approvals are required for this CHS pursuant to Section 5 (Special Approval Requirements) of this Manual [redacted] If the CHS is in a special approval category and is expected to provide purely criminal (and not national security/International Terrorism) information, then a lead must be sent to HIMU to notify the Human Source Review Committee (HSRC). [redacted] b7E

CHSs who are expected to report on national security/International Terrorism matters need not be referred to the HSRC.

2.2. Additional Information Required within First 90 Days of Opening

(U) The following information or requests for information [redacted] must be documented in the CHS's main file no later than 90 days after the opening date: b7E

- (U) All required and applicable instructions must be completed (prior to utilization/tasking but no later than 90 days after opening) and reviewed by the SSA during Quarterly SSA Source Report (QSSR) reviews (See Section 4.1, Instructions).
- (U) [redacted]
- (U) [redacted] including the same information required for [redacted] (See Section 2.1., Opening Communication) b7E
- (U) [redacted]
- (U) [redacted] b7E
- (U) [redacted]
- (U) [redacted]
- (U) Documentation showing that the Co-CA has met the CHS (this can be any documentation that reflects that the Co-CA has met with the CHS, e.g., Source reporting documents, payment receipts, instructions)
- (U) (~~S~~/NF) SAs may use their own discretion [redacted]

(U)

- (U) [redacted] b7E
- (U) [redacted]
- (U) [redacted]
- (U) [redacted]
- (U) [redacted] b7E
- (U) [redacted]
- (U) [redacted] if relevant and if possible to ascertain: [redacted]
- (S) [redacted] b1 b7E
- (U//FOUO) [redacted] b7E

(U) [redacted] (This guideline is not mandatory.)

2.3. Criminal Justice Information Services (CJIS) Division/NCIC "Stop Notices"

(U) [redacted] b7E

[6] (U) An émigré is a person who departs from his/her country for any lawful reason, with the intention of permanently resettling elsewhere.

[redacted] b7E

2.4. Positive Records Checks/Concurrence to Operate

(U) [redacted] the Agent attempting to open the CHS shall coordinate with the FO conducting the investigation. The resolution or concurrence to operate must be documented in the CHS's main file. b7E [redacted] then the CA must document that fact and the individual may be opened as a CHS. [redacted] 6.11. Also, an FPO may have to be notified (see Section 9.7.2., Notification to DOJ of Investigation or Prosecution).

2.5. Additional Requirements for Certain Confidential Human Sources

(U//FOUO) [redacted] b7E (See Section 5, Special Approval Requirements.)

(U//FOUO) Additionally, other CHSs may require approval from or notification to FBIHQ and/or someone outside of the FBI. Yet other CHSs may require that additional instructions be discussed at the CHS's opening. Some examples of CHSs that fall into these categories are: [redacted]

(S) [redacted] b1 b7E

(U) While the above listed types of CHSs are examples, more comprehensive guidance is found in Section 4, Instructions; Section 5, Special Approval Requirements; Section 6, The Development and Use of Sensitive Confidential Human Sources; Section 7, [redacted] and Section 8, [redacted] b7E

3. Confidential Human Source Validation

3.1. Validation

(U//FOUO) [redacted] The FBI should utilize [redacted] efforts, or reports. Every CHS shall be subject to the Confidential Human Source Validation Standards Manual (CHSVSM), which provides for a [redacted] at FBIHQ. For each CHS, CAs complete and submit a Field Office Annual Source Report (FOASR) to FBIHQ [redacted] in the appropriate FBIHQ operational division. Field division heads are responsible for establishing an appropriate [redacted] that includes [redacted] of FOASRs. Executive review of the FOASR can be delegated to an SSA. See the CHSVSM. b7E

(U//FOUO) [redacted] shall be promptly reported to an FBI Supervisor and then recorded and maintained in the [redacted] b7E

(U//FOUO) On a quarterly basis, a FO SSA conducts a QSSR for each CHS. QSSR [redacted] (See Section 16.9., Quarterly SSA [redacted]

(U//FOUO) All FOASRs shall be forwarded to the FBIHQ [redacted] in the appropriate FBIHQ operational division (i.e., [redacted] FBIHQ [redacted] determine the scope and extent of review. All CHSs would be subject to a [redacted] FBIHQ provides feedback to the FOs containing one of the following: Findings to Continue Operation, Findings to [redacted] or Findings to Close. An appeals process is detailed in the CHSVSM. b7E

(U//FOUO) [redacted] NSIGs, the FBIHQ [redacted] to the CHSVSM. The DI shall notify DOJ's National Security Division (NSD) within [redacted] of the FBIHQ's approval of the continued use of CHSs in the [redacted] The Assistant Attorney General (AAG) for the NSD shall designate FPO Attorneys [redacted] (See Section 5, Special Approval Requirements and the AGGs CHS.) b7E

4. Instructions to be Discussed with a Confidential Human Source

4.1. Instructions

(U//FOUO) The AGGs CHS require that at opening and thereafter at least annually or more often if circumstances warrant, at least one FBI Agent and a witness who is either another FBI Agent or other government official must advise the CHS of all applicable instructions detailed in this Manual (the advising Agent must be an FBI Agent). Recognizing that the opening process may take some time, the instructions must be discussed with the CHS at any time prior to the first operational use but no later than 90 days after the date of opening.

For purposes of delivering instructions to the CHS, the CHS is not considered opened by the FBI until [redacted]. In these situations, the file may be opened to maintain all requests and the file opening date will still be used as the original opening date for validation requirements. Once the outside approvals are obtained, the FBI Agent must deliver the instructions consistent with this Manual. The delivering FBI Agent and witness shall document that these instructions were given and that the CHS acknowledged the instructions and his/her understanding of them. The FBI Supervisor shall review such documentation at the QSSR review. Such documentation must be maintained in the CHS's main file. The content and meaning of the following provisions must be clearly conveyed: b7E

- The CHS's assistance and the information provided to the FBI are entirely voluntary.
- The CHS must abide by the instructions of the FBI and must not take or seek to take any independent actions on behalf of the U.S. Government.
- The CHS must provide truthful information to the FBI.
- The US Government will strive to protect the CHS's identity but cannot guarantee it will not be divulged.

4.2. Additional Instructions

(U//FOUO) If applicable to the particular circumstances of the CHS, or as they become applicable, the AGGs CHS require that additional instructions must be provided to the CHS, and the delivering FBI Agent and witness must document in the CHS's file that they have been provided and that the CHS acknowledged his/her receipt and understanding of the instructions. The content and meaning of the following instructions must be clearly conveyed:

- The FBI on its own cannot promise or agree to any immunity from prosecution or other consideration by an FPO, a state or local prosecutor, or a Court in exchange for the CHS's cooperation because the decision to confer any such benefit lies within the

exclusive discretion of the prosecutor and the Court. However, the FBI will consider (but not necessarily act upon) advising the appropriate prosecutor of the nature and extent of the CHS's assistance to the FBI. (This instruction should be given if there is any apparent issue of criminal liability or penalty.)

- [redacted] the CHS is not authorized to engage in any criminal activity and has no immunity from prosecution for any unauthorized criminal activity. [redacted] This instruction should be repeated if the CHS is suspected of committing unauthorized illegal activity. See Section 9.7.1., Notification to DOJ of Unauthorized Illegal Activity, and Section 10, CHS Participation in Illegal Activity.) b7E
- The CHS is not an employee of the U.S. Government and may not represent himself/herself as such except under those circumstances where the CHS has previously been, and continues to be, otherwise employed by the U.S. Government.
- The CHS may not enter into any contract or incur any obligation on behalf of the U.S. Government, [redacted] or under those circumstances where the CHS is otherwise authorized to enter into a contract or incur an obligation on the behalf of the United States. b7E
- [redacted]
- The FBI cannot guarantee any rewards, payments, or other compensation to the CHS.

Each time a CHS subject to the AGGs CHS receives any rewards, payments, or other compensation from the FBI, the CHS shall be advised at the time of payment that he/she is liable for any federal, state, or local taxes that may be owed on that compensation. All CHSs operating domestically (in any U.S. territory) and [redacted] (U.S.) case are subject to the AGGs CHS and must be provided this instruction. b7E

[redacted] b7E

4.2.3. [redacted]

[redacted] b7E

4.2.4. [redacted]

(U//FOUO) [redacted]

4.2.5. [redacted]

(U//FOUO) [redacted]

4.2.6. [redacted]

(U//FOUO) [redacted]

5. Special Approval Requirements

5.1. Special Approvals

(U) The AGGs CHS apply to all CHSs' domestic (U.S. territory) activity. The AGGs CHS apply [redacted] b7E
[redacted] All CHSs subject to the AGGs CHS must be evaluated to determine whether special approval for continued use by DOJ is required as follows:

(U) CHSs who are expected to report on criminal matters (and not on national security, including International Terrorism and other matters governed by the NSIGs and who do not already have an FPO involved) would be reviewed by a HSRC, a committee comprised of DOJ and FBI representatives that convenes pursuant to the AGGs CHS, if the CHS falls into any of the [redacted] These CHSs may be opened or approved for continued use by the FO's SSA; however, the FO must notify HIMU of all special approval category CHSs so that [redacted] can refer them to the [redacted] FOs must notify [redacted] on the opening communication and on the FOASR (or in writing any time the CHS's status changes thus making him/her subject to the HSRC review). Within 60 days of a CHS's utilization who falls into any of these categories (or within 60 days of FBIHQ's approval for continued use of [redacted] must seek written approval from the [redacted] for continued use unless an FPO attorney has existing oversight of a CHS because the CHS has agreed to testify in a federal criminal prosecution. However, [redacted] would be referred to the [redacted] regardless of whether the CHS has worked with an FPO). Relevant information concerning the use of the CHS, except for the identity of the CHS unless the Deputy Assistant Director (DAD) chairing the [redacted] in coordination with the FO's SAC determines that compelling reasons exist to warrant such a disclosure, shall be provided to the [redacted] The CHS may continue to be operated while such approval is pending. The [redacted] approval process shall be completed no more than 45 days after the FBI submitted the request. b7E

(U) CHSs who report on national security matters, including International Terrorism or other activities under the NSIGs are not reviewed by the [redacted] Rather, these CHSs would be reviewed by a DOJ Attorney designated by the AAG of DOJ's NSD. This review does not occur at opening. Instead, [redacted] of FBIHQ approving the continued use of a CHS who was subjected to the [redacted] of the [redacted] the DI provides notice to a designated FPO Attorney in the NSD (see Section 3.1. [redacted] AGGs CHS). Upon request from the NSD Attorney, the FBI shall make available at FBIHQ [redacted] NSD's objections to the continued use of the CHS would be forwarded to the Deputy Attorney General (DAG); however, the FBI would be allowed to utilize the CHS pending the resolution. The CHS's identifying information is not disclosed unless the Assistant b7E

Director (AD) or the DAD of the division using the CHS determines that compelling reasons warrant such a disclosure.

[redacted] b7E

[redacted] For additional information about these DOJ reviews and the further appeals process, see the AGGs CHS.

5.2. Special Approval Categories

(U) (S//NF) All requests seeking approval for the continued use of CHSs who meet any of the definitions in this Section [redacted] for criminal matters shall be submitted to [redacted] and then reviewed and approved by the [redacted] except when the FPO is involved with the CHS. This exception does not apply to [redacted] CHSs expected to report on International Terrorism or matters governed by the NSIGs are not referred to the HSRC (See Section 5.1, Special Approvals). Instead, these CHSs would be referred to DOJ's NSD after FBIHQ recommends continued use pursuant to an [redacted] b7E

5.2.1. [redacted]

[redacted] b7E

5.2.2. [redacted]

[redacted] b7E

(U//FOUO)

5.2.3.

b7E

5.2.4.

b7E

5.2.4.1.

5.2.4.2.

5.2.4.3.

b7E

5.2.4.4.

5.2.5.

5.2.6.

b7E

[redacted] b7E

[redacted] b7E

6. The Development and Use of Sensitive Confidential Human Sources

6.1.

b7E

6.1.1.

(U//FOUO) If an FPO is participating in the conduct of an investigation by the FBI in which a would be utilized as a CHS or would be working with such CHSs in connection with the prosecution, the FBI shall notify the FPO Attorney assigned to the matter prior to using the person as a CHS.

6.2.

(U//FOUO)

b7E

(U//FOUO)

[redacted] b7E

(U//FOUO) [redacted]

[redacted] (See Section 6.2.2., Written Approval Communication).

6.2.1. Additional Approvals to Utilize [redacted]

(U//FOUO) [redacted] b7E

(U//FOUO) However, OEO policy does not require OEO approval if:

- [redacted]
- [redacted] b7E

(U//FOUO) [redacted]

- [redacted]

- [redacted]
- [redacted]
- [redacted]

b7E

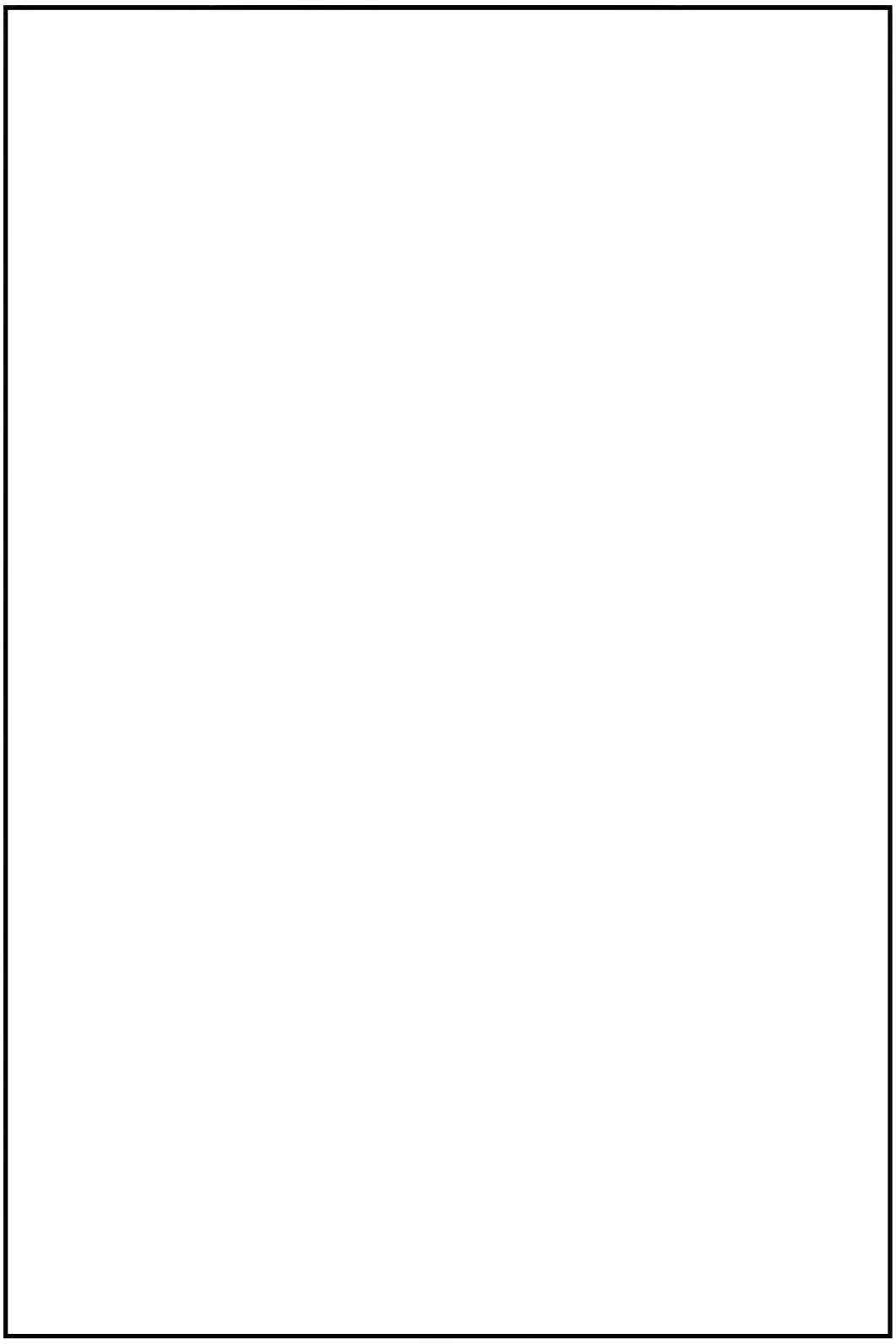
6.2.2. Written Approval Communication

(U//FOUO) The CA shall prepare a communication approved by the SAC to [redacted] which coordinates with the substantive unit and obtains OEO approval. If there are exigent circumstances, an immediate oral response can be obtained from OEO by FBIHQ with the written approval to follow. The communication to [redacted] uses the CHS's file number as the Case ID number. As required by OEO, the FO shall provide [redacted] with the following information in a Letterhead Memorandum (LHM) format appropriate for dissemination to OEO:

b7E

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

b7E



b7E

- [redacted]
- [redacted]
- [redacted]

[redacted] b7E

6.3. [redacted]

[redacted] b7E

6.3.1. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

b7E

(U//FOUO) [redacted]

6.3.2. [redacted]

b7E

(U//FOUO) If an FPO is participating in the conduct of an investigation by the FBI in which a [redacted] would be utilized as a CHS or would be working with a [redacted] in connection with the prosecution, the FBI shall notify the FPO Attorney assigned to the matter prior to using the person as a CHS.

6.4. [redacted]

(U//FOUO) [redacted]

b7E

- [redacted]
- [redacted]
- [redacted]

- [redacted]
- [redacted] b7E
- [redacted]
- [redacted]
- [redacted]
- [redacted]

6.5. [redacted]

[redacted]

6.6. [redacted] b7E

[redacted]

6.7. [redacted]

[redacted]

- [redacted]
- [redacted] b7E
- [redacted]
- [redacted]

- [redacted]
- [redacted]

6.8. [redacted] b7E

(U//FOUO) A court order is required before [redacted] if he/she is going to provide information on either employees of, or patients in, such a program (see 42 Code of Federal Regulations Section 2.67). If the individual is being opened for the purpose of obtaining information unrelated to his/her employment, employees, or [redacted] then this fact shall be documented to the CHS's main file, and a court order is not required.

6.9. [redacted]

(U//FOUO) The FBI may accept information concerning alleged violations of law or other matters within FBI jurisdiction from [redacted] The FBI may not target CHSs for the sole purpose of collecting information concerning the political beliefs or personal lives of individuals [redacted] will not knowingly influence or attempt to influence any action of a [redacted] unless in furtherance of a compelling governmental interest. If the investigation plans any activity which may [redacted] the CA must consult with the CDC. b7E

6.10. [redacted] b1 b7E

(S)

(U//FOUO) [redacted]

(U//FOUO) [redacted] b7E

(U//FOUO) [redacted]

6.10.1. FO Responsibility

(U//FOUO) The FO must send an Electronic Communication (EC) to the [redacted] at FBIHQ [redacted] then prepares a [redacted] b7E

- Full name (First, Middle, Last)
- Date-of-birth
- Place-of-birth
- SSAN
- [redacted] b7E
- Anticipated CHS activities/tasking
- The results of the completed background investigation
- FBI point-of-contact and [redacted]

6.10.2. FBIHQ Responsibility

(U//FOUO) Upon receipt of the FO's EC, HIMU coordinates with the substantive unit and [redacted] b7E

(U//FOUO) [redacted]

- The results of FBIHQ indices checks
- A request for concurrence in the utilization of the person as a CHS
- [redacted] b7E

(U//FOUO) [redacted]

- The results of FBIHQ indices checks
- [redacted]

(U//FOUO) [redacted] b7E

[redacted]

- The results of FBIHQ indices checks
- A request for concurrence in the utilization of the person as a CHS
- [redacted]
- [redacted] b7E

(U//FOUO) [redacted]

[redacted]

6.11. [redacted]

(U//FOUO) A [redacted] is an individual:

- For whom [redacted]
- For whom a [redacted] and b7E
- For whom the [redacted] is willing, if necessary, to seek his/her [redacted]

(U//FOUO) The CA may communicate with a current or former CHS who is a [redacted] only if:

- The communication is part of a legitimate [redacted]
- The [redacted] CHS initiates the communication; or
- Approved, in advance whenever possible, by a Supervisor of any federal, state, or local law enforcement agency that has a [redacted] b7E

(U//FOUO) An SA who communicates with a [redacted] must promptly report such communication to the SSA and to the appropriate federal, state, or local enforcement agency [redacted] and document that communication in the CHS's file.

6.12.

(U//FOUO) To open a CHS, a detailed justification explaining the reason this individual requires the protection of the FBI's CHS program must be presented to the SAC and approved prior to opening (this approval requirement may not be delegated). All instructions apply if opened as CHSs.

(U//FOUO) SSA approved payments to are restricted to reimbursements for expenses incurred in direct support of an investigation and relocation expenses if justified and necessary. Compensation to these individuals for services as a CHS, to include lump sum payments, must be approved by the SAC (this approval may not be delegated). The CA should consult with the CDC who may confer with the Office of the Chief Acquisition Officer, Finance Division (FD) at FBIHQ to determine whether a should be used. If applicable, an FPO Attorney participating in the conduct of the investigation must be consulted regarding these payments. b7E

(U//FOUO) that person to Generally, contact the at FBIHQ. See Section 6.13. in the CHSPM. See Section 11.8 in the Undercover Operations Manual, NFIPM, Section 28, and Sections II.C and III in the AGGs for

6.13.

(U//FOUO) When considering the use of CHSs or any individual in consult with the FO's UC Coordinator and/or with the at FBIHQ for either criminal or national security matters. If an individual meets the definition of an in this Manual), that person must not be designated as a CHS. Instead, the person must be designated as an Further, if an individual meets neither the definition nor the requirements to be designated as an FBI CHS, the b7E

(U//FOUO) If it is necessary for a CHS to be involved in an operation covered by the the activity requires approval by the Further, any investigation which potentially involves sensitive circumstances as defined by the must be referred to the FO's CDC for review before SAC approval is granted for the CHS to participate in

the investigation. The CDC's assessment and SAC's approval must be documented in the CHS's main file.

(S) [redacted] b1

6.14. [redacted]

(U//FOUO) The FBI's issuance of an [redacted] is only allowed in extraordinary circumstances in accordance with the following policy:

b7E

(U//FOUO) If the individual qualifies as [redacted] then the CHS must be closed and designated as [redacted] instead. This may constitute an [redacted] For additional information, [redacted] or see the [redacted] (See Section 6.12.) [redacted]

(U//FOUO) If, however, the CHS does not [redacted] the FO may request that [redacted] be issued to the CHS. Because [redacted] to a CHS constitutes an extraordinary circumstance, these requests are only granted under limited situations. The CA must submit a written communication, approved by the SAC and [redacted] the appropriate substantive unit, the appropriate FBIHQ [redacted] and the [redacted] that the CHS could not be designated as an [redacted] could not be issued [redacted] The written justification must detail the reason(s) the CHS requires an [redacted] following the procedures detailed in this Manual.

b7E

(U//FOUO) As an extraordinary request, approval lies within the discretion of FBIHQ and is not guaranteed. Approval for [redacted] must be granted by the Section Chief responsible for the CHS Program (this authority may not be delegated). Other approvals are required by the policies of the substantive division(s) and [redacted] coordinates all FBIHQ approvals and notifies the FO of the final decision.

(U//FOUO) [redacted] b7E
The FO must utilize other methods to provide protection. [redacted]

(U//FOUO) If an [redacted] the FO is responsible for complying with all guidance from the [redacted]

6.15. [redacted]

(U//FOUO) [redacted] b7E

[redacted]

6.16. [redacted]

(U//FOUO) If the CHS is an [redacted] the FO must notify [redacted] personnel of this fact. [redacted] notifies the AD of the substantive division and the substantive unit. If the AD has questions or concerns about the opening of the CHS, the AD may contact the FO or the substantive unit to resolve the issues. b7E

6.17. [redacted]

(U//FOUO) [redacted] b7E

[redacted]

(S)

(S)

[redacted] b1 b7E

8. Immigration

8.1.

b7E

8.1.1. FBI Policy

(U//FOUO) It is the policy of the FBI to attempt to the status of a CHS who is known to be an

8.1.2. Requirements

(U//FOUO) The SSA must authorize the opening of an and that authorization must be documented in the CHS's main file.

b7E

(U//FOUO)

b7E

(U//FOUO) If a determination is made to close the CHS

b7E

(U//FOUO) coordinates these matters with the substantive divisions at FBIHQ as necessary.

8.1.3. Operation

(U//FOUO)

(U//FOUO)

b7E

(U//FOUO)

b7E

(U//FOUO)

8.2.

(U//FOUO)

b7E

(U//FOUO)

(U//FOUO)

(U//FOUO)

b7E

(U//FOUO) To initiate a request for either FOs shall provide the following information after SAC approval t

Requests for must be on a DOJ supplemental

- Significance of the investigation
- Significance of cooperation
- Basis of request of [redacted] status
- [redacted] (if applicable)
- Assessment of threat to the witness
- Pre-existing grounds of excludability (i.e., pending criminal charges)

(U//FOUO) [redacted]

- [redacted]

b7E

(U//FOUO)

b7E

(U//FOUO) Upon the initial submission of the application to DOJ,

(U//FOUO)

are effective tools for law enforcement and intelligence operations that involve

b7E

CHS, i.e., name, alien number, sex, date-of-birth, and country-of-birth). All NCIC, and

8.3.

(U//FOUO)

b7E

(U//FOUO) To initiate a request, FOs should contact or check the DI Intranet site for examples of the way to document the request and for current application procedures to obtain

(U//FOUO) are the responsibility of the sponsoring FO. FOs must make their best effort to ensure that these individuals do not violate any US laws while they are The CA

b7E

8.4.

(S)

b1
b7E

8.5.

(U//FOUO) is an administrative remedy of the last resort to and as such, all appropriate administrative relief should be exhausted before considering deferred action. does not confer for any purpose

b7E

[redacted] b7E

(U//FOUO) To initiate a [redacted] request, FOs should contact [redacted] or check the DI intranet site for ways to document the request and to access current application procedures to request deferred action.

8.6. [redacted]

(U//FOUO) [redacted] granted by the District Director for ICE's District Office, after consultation with DOS, on the basis of whether [redacted] b7E

(U//FOUO) [redacted]

(S) [redacted] b1 b7E

9. Utilization of Confidential Human Sources

9.1. Confidential Human Sources Who Testify in a Court or Other Proceeding

(U//FOUO) Whenever it becomes apparent that a CHS may have to testify in a court or other proceeding, the CA must advise the CHS of that possibility. This advisement must be documented in the CHS's main file. Additionally, written documentation of FPO concurrences with certain aspects of further CHS operation, which may be at issue in court, must be documented in the CHS's main file (e.g., payments, Tier I illegal activity).

(U//FOUO) If the CA gives the CHS instructions to gather physical or documentary evidence or make consensual recordings which will be used in trial, that CHS may be required to testify, and the CHS should be informed by the CA prior to the tasking.

(U//FOUO) Unanticipated situations may arise, however, that cause a CHS to testify even though the CHS has not previously agreed to do so. For example, [redacted] it may be necessary for the CHS to testify. If there is a possibility that a Court may require a [redacted] b7E

9.2. [redacted]

(U//FOUO) [redacted] must comply with the Attorney General's Procedures for [redacted]. Per FBI policy [redacted] requires SAC approval. CDC concurrence is required for sensitive circumstances as outlined in the [redacted] The CA shall ensure that all appropriate documentation required for [redacted] b7E
The FO is required to maintain records for each [redacted] that it has conducted. DOJ approval is also required (see below).

(U//FOUO) The CDC may review requests for [redacted] for privilege issues, evidentiary issues, issues involving represented persons, and similar legal considerations based on current case law. The CA should consult with the CDC for guidance any time such issues or concerns arise.

(U//FOUO) In sensitive circumstances as defined by the [redacted] written approval from DOJ/OEO is required. The FO sends the [redacted] request to the substantive unit, which obtains OEO approval and notifies the FO of such. In non-sensitive circumstances, the FO obtains oral approval from a DOJ attorney, either an AUSA or an attorney from the Criminal Division of DOJ, designated by the AAG. However, if the investigation is being conducted pursuant to the NSIGs, then DOJ approval is not required. Instead, only the CDC's or OGC's approval is required. In national security investigations, Agents should consider consulting with FPO/DOJ Attorneys if any are assigned.

(U//FOUO) In exigent circumstances, when DOJ approving officials can not be reached, authorization may be given by the SAC or ASAC. In this situation, the FO must notify the substantive unit. The substantive unit then must notify OEO as soon as practical, but no later than three working days after the approval.

(U//FOUO) The CHS must be present at all times to ensure the [redacted] If the CHS makes a [redacted] that at the time is intended to be used in court, the CHS must have agreed to testify. [redacted] in which a CHS may be present should consider whether that CHS has agreed to testify. Documentation of the CHS's agreement to testify must be in the CHS's main file. b7E

9.3. [redacted]

(U//FOUO) [redacted]

9.4. Obtaining Information about a [redacted]

(U//FOUO) If a [redacted] who is facing pending criminal charges for which his/her Sixth Amendment right to counsel has attached, the [redacted] regarding the pending charges. A subject's Sixth Amendment right attaches when a prosecution is commenced (i.e., at or after the initiation of adversarial judicial criminal proceedings—whether by way of formal charge, preliminary hearing, indictment, information, or arraignment). b7E

(U//FOUO) Nevertheless, a CHS may be directed to: [redacted]

(U//FOUO) In certain circumstances, a [redacted] but against whom charges are not pending may be limited by other laws (see the Citizen's Protection Act codified at 28 USC § 530B). On any occasion when [redacted] it is recommended that the CA consult with the FO's CDC. b7E

(U//FOUO) Finally, a CHS should be instructed not to interfere with the subject's attorney/client relationship. For example [redacted]

9.5. Confidential Human Sources

(U//FOUO) Using a CHS to [redacted] b7E
[redacted] The CA cannot accept communication contents and records in violation of the Electronic Communications Privacy Act (ECPA). Court orders may be required to obtain such information. Guidance on these issues may be provided by the substantive unit, CDC, OGC, the Cyber Division, and any relevant FPO.

9.6. Information from [redacted]

(U//FOUO) [redacted] are individuals from whom [redacted] The CHS [redacted] reports the information directly to the CA. [redacted] are not [redacted] are not operated at the direction of the FO, and cannot be controlled by the FBI. Additionally, [redacted] b7E
[redacted] Therefore, in order to prevent intelligence from being mistakenly disseminated within the Intelligence Community with the impression that it is derived from a [redacted] the information must be appropriately attributed [redacted] whose reliability is unknown. CHS reporting must accurately describe the reliability of the information or its origin.

9.7. Special Notification of Information to DOJ

9.7.1. Notification to DOJ of Unauthorized Illegal Activity

(U//FOUO) If an FBI Agent has reasonable grounds to believe that a CHS has engaged in unauthorized criminal activity (other than minor traffic offenses), the FBI shall promptly notify DOJ's CHSC or the assigned FPO Attorney. In turn, the DOJ's CHSC or assigned FPO Attorney shall notify the following FPOs of the CHS's criminal activity and his/her status as a CHS:

- The FPO in whose district the criminal activity primarily occurred, unless a state or local prosecuting office in that District has filed charges against the CHS for the criminal activity and there is no basis for federal prosecution in that District;
- The FPO Attorney, if any, who is participating in the conduct of an investigation that is utilizing the CHS or who is working with the CHS in connection with a prosecution; and
- The FPO Attorney, if any, who authorized the CHS to engage in OIA.

(U//FOUO) Whenever such notifications are provided, the CFP and the FBI SAC, with the concurrence of each other, shall notify any state or local prosecutor's office that has jurisdiction over the CHS's criminal activity and that has not already filed charges against the CHS for the criminal activity of the fact that the CHS has engaged in such criminal activity. The CFP(s) and the SAC(s) are not required, but may, with the other's concurrence, also notify the state and local prosecutor's office of the person's status as a CHS. These notifications should be documented in the CHS's file.

(U//FOUO) If the SAC determines that the CHS will continue to be utilized, then an FBI Agent shall re-admonish the CHS that he/she is not authorized to participate in an illegal activity and has no immunity for participation in such unauthorized illegal activity. This admonishment should be witnessed by another FBI Agent, government official, and/or TFO. The admonishment must be documented in the CHS's file consistent with the requirements in Section 4.1., Instructions.

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirements.

9.7.2. Notification to DOJ of Investigation or Prosecution

(U//FOUO) If an FBI Agent has reasonable grounds to believe that the alleged felonious activity of a current or former CHS is, or is expected to become, the basis of a prosecution or investigation by an FPO or a state or local prosecutor's office, the FBI Agent must immediately notify a DOJ CHSC or the assigned FPO Attorney of that individual's status as a current or former CHS. However, with respect to a former CHS whose alleged felonious activity is, or is expected to become, the basis of a prosecution or investigation by a state or local prosecutor's office, no notification obligation shall arise unless the FBI Agent has reasonable grounds to believe that the CHS's prior relationship with the FBI is material to the prosecution or investigation.

(U//FOUO) Whenever such a notification occurs, the DOJ's CHSC or the assigned FPO Attorney shall notify the CFP. The CFP and the FBI SAC, with the concurrence of each other, shall notify any other federal, state, or local prosecutor's office or law enforcement agency that is participating in the investigation or prosecution of the CHS.

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirements.

9.7.3. Notification to DOJ Regarding Certain Federal Judicial Proceedings

(U//FOUO) The FBI shall immediately notify an appropriate DOJ CHSC or the assigned FPO Attorney whenever an FBI Agent has reasonable grounds to believe that:

- A current or former CHS has been called to testify by the prosecution in any federal grand jury or judicial proceeding;
- The statements of a current or former CHS have been, or will be, utilized by the prosecution in any federal judicial proceeding; or
- An FPO Attorney intends to represent to a Court or jury that a current or former CHS is or was a co-conspirator or other criminally culpable participant in any criminal activity.

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirements.

9.7.4. Notification to DOJ of Privileged or Exculpatory Information

(U//FOUO) If an FPO is participating in the conduct of an investigation by the FBI that is utilizing a CHS or working with a CHS in connection with a prosecution, the FBI shall notify the FPO Attorney assigned to the matter, in advance whenever possible, if the FBI has reasonable grounds to believe that the CHS will obtain or provide information that is subject to, or arguably subject to, a legal privilege of confidentiality belonging to someone other than the CHS.

(U//FOUO) Whenever (regardless of whether an FPO is assigned or participating in the conduct of a related investigation) an FBI Agent knows or reasonably believes that a current or former CHS has information that is exculpatory as to a target of a federal, state, or local investigation, or as to a defendant (including a convicted defendant) in a federal, state, or local case, the FBI Agent shall disclose the exculpatory information to either the assigned FPO Attorney that is participating, or had participated, in the conduct of that investigation or to the DOJ CHSC.

(U//FOUO) In turn, the assigned FPO Attorney or the DOJ CHSC shall disclose the exculpatory information to all affected federal, state, and local authorities. In the event the disclosure would jeopardize the security of the CHS or seriously compromise an investigation, the FPO Attorney or the DOJ CHSC shall refer the matter to the HSRC for consideration, except such matters with respect to an International Terrorism investigation, national security investigation, or other activity under the NSIG shall be referred to the AAG of the NSD or his/her designee.

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirements.

9.7.5. [redacted]

(U//FOUO) The FBI shall not [redacted]

- [redacted] would endanger that person's life or otherwise jeopardize an ongoing investigation; or b7E
- [redacted] based on his/her suspected involvement in unauthorized criminal activity.

(U//FOUO) In the event the [redacted] the CA must inform the FPO Attorney making the application and the Court to which the application is made [redacted]

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirement.

(S) **9.7.6.** [redacted]

(S) [redacted] b1 b7E

- Whether or not the CHS was paid. This can be done using general terms so that no exact amounts are given (e.g., the CHS was paid a modest fee for information).
- [redacted]
- Any other Brady/impeachment information.

(U//FOUO) Agents are encouraged to consult with the CDC and/or the National Security Law Branch (NSLB) regarding details of the above information.

9.7.7. Responding to Requests from FPO Attorneys Regarding a Confidential Human Source

(U//FOUO) In any criminal matter arising under, or related to, the AGGs, upon request by an appropriate FPO Attorney, the FBI shall promptly provide the FPO Attorney all relevant information concerning the CHS, including whether he/she is a current or former CHS for the FBI.

(U//FOUO) If the FBI SAC has an objection to providing such information based on specific circumstances of the case, he/she shall explain the objection to the FPO making the request and any remaining disagreement as to whether the information should be provided shall be resolved pursuant to Section 20, Exceptions and Dispute Resolution of the AGGs CHS.

(U//FOUO) See Section 9.7.8., Exceptions to the Special Notification Requirements, for exceptions to the FPO DOJ notification requirements.

9.7.8. Exceptions to the Special Notifications Requirements

(U//FOUO) The Director of the FBI, with the written concurrence of the DAG, may withhold any notification required pursuant to the following sections of this Manual: Section 9.7.1., Notification to DOJ of Unauthorized Illegal Activity; Section 9.7.2., Notification to DOJ of Investigation or Prosecution; Section 9.7.3., Notification to DOJ Regarding Certain Federal Judicial Proceedings; Section 9.7.4., Notification to DOJ of Privileged or Exculpatory Information; Section 9.7.5.[redacted] b7E [redacted] and Section 9.7.7., Responding to Requests From FPO Attorneys Regarding a CHS. Such concurrence must be based on a determination that the identity, position, or information provided by the CHS warrants extraordinary protection

for sensitive national security reasons. Any such determination to withhold notification shall be documented and maintained in the CHS's main file along with the concurrence of the DAG.

9.7.9. DOJ Review of FBI Confidential Human Source Files

(U//FOUO) If the FBI discloses any information about a CHS to an FPO Attorney pursuant to Sections 9.7.1., 9.7.2., 9.7.3., 9.7.4, 9.7.5., and 9.7.7., the SAC and the CFP shall consult to facilitate any reviewing and copying of the CHS's files by the FPO that might be necessary for an FPO Attorney to fulfill his/her disclosure obligations.

9.7.10. Designees

(U//FOUO) An SAC and a CFP may, with the concurrence of each other, designate particular individuals in their respective offices to carry out the functions assigned to them in paragraphs 9.7.1. – 9.7.9., excluding 9.7.8., Exceptions to the Special Notification Requirements.

10. Confidential Human Source

10.1.

(U//FOUO)

b7E

- b7E

b7E

- [redacted]
- [redacted] b7E

[redacted]

10.2. Authorization Requirements

(U//FOUO) The SAC or ASAC (see Section 10.5., Designee Section) must authorize all [redacted] by an FBI CHS and the authorization, and all subsequent re-authorizations, must be documented in the CHS's file (see Section 10.11, Record Keeping Procedures). b7E

[redacted]

[redacted] b7E

10.3. [redacted]

[redacted] b7E

- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted] b7E
- [redacted]
- [redacted]
- [redacted]

10.4. [redacted] b7E

[redacted]

10.5. Designees

(U//FOUO) The FBI SAC and the CFP may agree to designate particular individuals at the supervisory level in their respective offices to carry out the approval functions assigned to them. However, this FBI policy provides that the SAC may not [redacted] approval authority to any position lower than ASAC. b7E

10.6. Emergency Authorization

(U//FOUO) In exceptional circumstances, the SAC [redacted] and the [redacted] without complying with the documentation requirements when they determine that a highly significant and unanticipated investigative opportunity would be lost were the time taken to comply with these requirements. In such an event, the documentation requirements, as well as written justification for the oral authorization, shall be completed [redacted] or as soon as practicable, of the oral approval and maintained in the CHS's file. b7E

10.7. [redacted]

[redacted]

- [redacted] b7E

[redacted] b7E

10.10. Renewal and Expansion of Authorization

(U//FOUO) If the FBI seeks to [redacted] for an additional time after the expiration of the authorized time period or after revocation of authorization, or if the FBI seeks to expand the scope of any CHS's [redacted] then the FBI shall document the circumstances of the renewal and/or expansion and must seek the appropriate level of [redacted] See Section 10.2, Authorization Requirements. b7E

10.11. Record Keeping Procedures

(U//FOUO) The FBI shall [redacted] (Although the AGGs CHS [redacted] tracked and reported annually to DOJ.) FOs shall [redacted] in a separate sub-file for more accurate accounting measures. FOs should be prepared to provide such information upon request. b7E

(U//FOUO) At the end of each calendar year, the FBI shall report to the AAG of the Criminal Division and the NSD the total number of times each FBI FO authorized a CHS [redacted] the overall nationwide totals.

(U//FOUO) If requested, the FBI shall provide to the AAG of the Criminal or NSD a copy of any written authorization, finding, or instruction [redacted]

11. [redacted]

b1
b7E

11.1. Requirements

(S) [redacted]

11.1.1. Field Office

(U//FOUO) SSA approval for the initiation and continuation of [redacted] must be obtained and documented in the CHS's main file.

b1
b7E

(S) [redacted]

11.1.2. Substantive Unit

(S) [redacted]

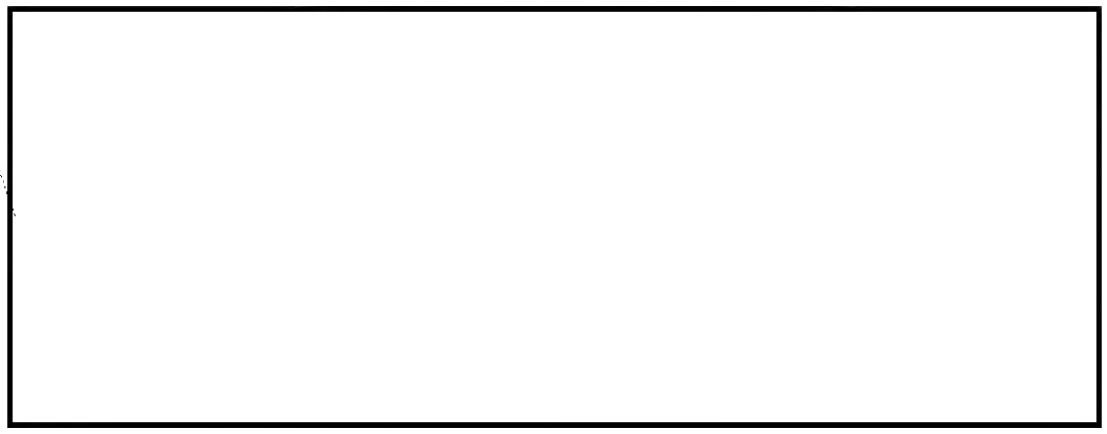
(U) (~~S~~//NF) If the Legat has questions or concerns about the contact, the substantive unit must coordinate between the FO and the Legat to address the concerns. Also, the substantive unit must obtain FBIHQ approval, as required. The substantive unit shall advise the FO when all appropriate approvals are obtained and notifications/concurrences are complete.

b1

(S) ~~11.1.3. Legat [redacted] Notification~~

(S) [redacted]

(S)



b1
b7E

11.1.4. Documentation

(S) (U//FOUO) Substantive unit and Legat approvals notifications as required must be documented. All to and from the CHS must be placed in the CHS's main file. Any intelligence information within must be reported in a manner that does not tend to identify the CHS and placed into the appropriate sub file.

b1
b7E

11.1.5. Security

(U//FOUO) When with a CHS, consideration should be given to the extent possible through the use of Additional guidance can be provided by the substantive divisions or through the at FBIHQ.

b7E

12. Domestic Travel

(U//FOUO) The SAC or designee may authorize operational travel between FOs by a CHS with the concurrence of the SAC or designee of the FO covering the location to be visited. The concurrences of all relevant FOs should be documented in the CHS's main file.

13. Operational Travel

(S)

b1
b7E

(U//FOUO) The DOJ and FBI are currently revising all
When these new AGGs CHS become available, they will be included in the Manual as

14. Joint Operation with Federal, State, Local and Tribal Agencies

14.1. Primary Responsibility

(U//FOUO) CHSs may be worked with any other government agency or with another FBI FO (see Section 15, Dissemination and Disclosure of the CHS's Identity). If the FBI is directing the CHS or if the CHS is primarily supporting an FBI investigation, the operation of and information from the CHS must comply with FBI instructions and be subjected to the FBI validation process.

(U//FOUO) FBI Agents have the primary responsibility for the operation of an FBI CHS, unless control of the CHS has been turned over to another agency for [redacted] Factors to consider to determine whether the FBI has control of a CHS are as follows: whether the FBI or other agency serves as the CHS's primary point of contact while outside the United States; the degree of contact the CHS maintains with the FBI; whether the FBI pays for the travel or related expenses; whether the FBI is directly tasking the CHS; and whether the particular operation of the CHS primarily supports a specific FBI investigation. [redacted] b7E

(U//FOUO) If the CA is unavailable, either the CA, Co-CA, or the SSA may designate, on a temporary basis, another SA to handle CHS operation and administration. Ultimately, the CA is responsible for the maintenance and accuracy of the CHS's file. Originals or copies of all records available to the FBI regarding CHS reporting, payments, and administrative matters must be maintained in FBI files. The CA must make reasonable efforts to determine whether the CHS was paid by any other agency.

14.2. Joint Operations [redacted] b7E

(U//FOUO) For joint operations [redacted] see the [redacted]

14.3. Joint Operations with Multiple FBI FOs

(U//FOUO) A CHS may work jointly with two or more FBI FOs. If the CHS resides, moves, or works in another FO's territory, then the CHS must have documented concurrence from all of the involved FOs' SACs or designee. The Office of Origin (OO) must notify the other FO of the CHS's opening and the area of anticipated reporting. The CA and Co-CA may be located in different offices. The OO is responsible for maintaining the file and, if jointly operated, the other office must designate copies of all reports of information received from the CHS, as well as any required documentation (e.g., payment information and receipts), to the OO file. Similarly, both offices must keep the other apprised of information impacting the FO's investigative programs, as well as

any change in the status of the CHS. To make payments to the CHS being operated by another FO, see Section 17.10., Payments to CHSs by Other Field Offices.

14.4. TFO as Co-Case Agent

(U//FOUO) The SSA of the OO may authorize an official from an outside agency who has been detailed to an FBI task force to act as a Co-CA. A TFO, however, may not be a CA. In those instances in which a CHS is referred to the FBI by a TFO, that fact must be indicated in the CHS's opening communication.

(U//FOUO) TFOs that have been authorized to act as a Co-CA may be present at CHS debriefings, may be present when payments are made to the CHS, and may have access to the CHS's file. A non-FBI Co-CA may meet with a CHS without being accompanied by an FBI Agent, provided that each such contact is fully documented by the TFO and placed in the CHS's file. However, an FBI Agent must witness all CHS payments that derive from FBI funds. Pursuant to the AGGs CHS, instructions (see Section 4, Instructions) must be completed by at least one FBI Agent.

14.5. TFO Co-Case Agent Responsibilities

(U//FOUO) Any TFO who has been designated as a Co-CA must be advised of and follow all relevant FBI policies regarding the development and operation of FBI CHSs as described in this manual.

15. Dissemination and Disclosure of the Confidential Human Source's Identity

15.1. Policy

(U//FOUO) Protection of a CHS's identity is of primary importance and disclosure should only be approved when it is absolutely necessary to achieve important investigative, public policy, and safety goals. FBI policy requires that the CHS's identity and relationship with the FBI be protected from disclosure except to those who need to know this information in order to carry out their official duties and except as legally required. This policy is firmly recognized in federal law and the FBI will do everything within its lawful authority to enforce the policy.

15.1.1. Approvals for Disclosure of a Confidential Human Source's Identity

(U//FOUO) SAC approval is required to disclose the identity of a CHS.

(U//FOUO) Notwithstanding any other provision, SAC approval is not required for:

- FBI SAs to disclose the identity of the CHS to other FBI SAs who have a need-to-know
- DOJ personnel to make appropriate disclosures when the CHS has agreed to testify in a grand jury or judicial proceeding
- Any DOJ personnel, which includes FBI employees, to disclose the identity of the CHS when required by court order, law, regulation, the AGGs CHS, or other DOJ policies

(U//FOUO) For the purposes of this section, SAC authority to disclose the identity of a CHS may be accomplished through the delegation of authority to an SSA to approve operational or administrative requests that by their very nature require disclosure of a CHS's identity (e.g., [redacted] b7E [redacted] Approval of operational or administrative requests also serves as documentation of authorization to disclose the CHS's identity, and no separate documentation is required.

(U//FOUO) Disclosures to anyone not included in the above operational or administrative approvals require prior SAC approval. Approvals must be documented in the CHS's main file.

(U//FOUO) No one to whom disclosure has been made is authorized to make further disclosures of the CHS's identity except when required by court order, law, regulation, AGGs CHS, or other DOJ policies.

(U//FOUO) Anyone making a disclosure has the responsibility to advise the recipient of the information that further disclosures or contact with the CHS is not authorized without the expressed consent of the FBI.

15.2. Required Disclosure to an FPO

(U//FOUO) If the FBI presents a case for prosecution and a CHS is expected to or may testify, the SA must reveal the identity of the CHS to the prosecutor. Pursuant to the AGGs CHS, FPOs must coordinate with the handling agent of the CHS in order to obtain SAC approval prior to revealing the identity of the CHS to any additional third party unless otherwise required by law or policy.

15.3. Responding to Requests from FPOs

(U//FOUO) In any criminal matter arising under, or related to, the AGGs, upon request by an appropriate FPO Attorney, the FBI shall promptly provide the FPO Attorney all relevant information concerning the CHS, including whether he/she is a current or former CHS for the FBI.

(U//FOUO) If the FBI SAC has any objection to providing such information, see Section 9.7.7., Responding to Requests from FPO Attorneys Regarding a CHS and Section 9.7.8., Exceptions to the Special Notifications Requirements.

15.4. Record of Information Dissemination or Disclosure of Identity

(U//FOUO) Identifying information about a CHS shall not be disclosed without proper approvals or as required by law. Potentially identifying information or identifiers shall be redacted if contained on a document that is disseminated, unless disclosure of the dissemination is approved.

(U//FOUO) A record of the dissemination of any CHS reporting should be maintained in the CHS's file to include the name of the person or agency to which the information was disclosed and a description of the information disclosed. This documentation may be completed on a statistical accomplishment form noting the file and serial number of the disseminated information or description of the information that was disclosed. If an Intelligence Information Report (IIR) was disseminated, then the IIR number alone will suffice. Dissemination of reporting information is encouraged and should be made to law enforcement, IC, or tribal authorities with proper clearance and a need-to-know.

(U//FOUO) The fact that the CHS's reporting was utilized in a court document must be documented. If the CHS testified in a court proceeding, this fact must also be documented. A statistical accomplishment form may be used to document this fact. If a statistical accomplishment form is used, then no other form of documentation would be required.

15.5. Legally Required Disclosure

(U//FOUO) All DOJ personnel must disclose the identity of a CHS, and the information that the CHS has provided, when required by court order, law, regulation, AGGs CHS, or other DOJ policies. DOJ personnel may make appropriate disclosures when the CHS has agreed to testify in a grand jury or judicial proceeding. If time permits, in response to any subpoena, court order, or request bearing on the identification of a CHS or the production of any part of a CHS's file, the SAC may seek to determine whether an attempt should be

made to assert appropriate administrative or legal objections to the request, demand, or order. In matters involving national security and other situations as appropriate, a request may be made to have the CHS's file reviewed in camera by a judge. In certain circumstances, the FBI may refuse disclosure of either the CHS's identity or information provided by the CHS. Such an action could result in the dismissal of the pending prosecution and must be coordinated with appropriate officials from the FPO. Any decision to withhold CHS information shall be coordinated with the appropriate FPO and decisions must be documented in the CHS's main file.

16. Administration of Confidential Human Sources

16.1. [redacted] b7E

[redacted]

16.2. Files

(U//FOUO) The [redacted] in the CHS's main file. [redacted] b7E

[redacted] Information not reported on an FBI form or that cannot be uploaded should be placed into [redacted]. Documents containing [redacted] must be filed in the [redacted] copies filed in the appropriate [redacted] if necessary.

(U//FOUO) CHS files have been designated by the National Archives and Records Administration for permanent retention. Therefore, records relating to CHSs cannot be deleted or destroyed. Additional guidance or information regarding the retention of these records can be obtained from [redacted] b7E

16.3. [redacted]

(U//FOUO) [redacted] or has intelligence value, whether received orally or otherwise, [redacted] from the CHS's [redacted] CHS (e.g., [redacted] Examples of personal information include the CHS's [redacted]

(U//FOUO) If information provided by the CHS is intelligence or is testimonial in nature, it must be reported on a CHS [redacted] CHS reporting documents [redacted] b7E
CHS reporting documents shall be appropriately classified and filed in the CHS's sub-file and appropriate substantive case files.

(U//FOUO) Information not obtained from the CHS's reporting (e.g., Agent observations, taskings, disclosures of information to the CHS) must be documented on a [redacted] in the CHS's file.

(U//FOUO) All FBI personnel must exercise due diligence to avoid disclosing information to a CHS other than what is necessary and appropriate for operational

reasons. If it is operationally necessary to disclose confidential investigative information to a CHS, then a [redacted] shall be used to document the information that is disclosed. Contact report forms must be filed in the [redacted]

16.4. Co-Case Agent Responsibilities

b7E

(U//FOUO) SAs that have been authorized to act as a Co-CA [redacted] may complete all other administrative duties for the CHS; and may [redacted] The Co-CA may meet with a CHS [redacted] FBI SAs who serve as Co-CAs have all the same duties and responsibilities as the CA.

16.5. Responsibility for Confidential Human Source Debriefing

(U//FOUO) Responsibility for handling and debriefing FBI CHSs, gathering evidence and intelligence from CHSs, and generating documents based on those activities is the FBI's CA responsibility. However, there may be times when the CA is unavailable to attend debriefings, etc. of the CHS. Therefore, the Co-CA, TFOs, and Agents/officers from other government agencies that may be operating the CHS jointly with the CA may debrief the CHS and report on the information obtained. Generally, analysts who participate in debriefings should not be put into positions that cause them to be the primary or only alternate fact witness concerning the information generated from the CHS.

16.6. [redacted]

b7E

(U//FOUO) CAs must assign [redacted] within the FO. The [redacted] The assignment of the [redacted] must be documented in the CHS's main file. It should not appear in any disseminable document except for communications to DOJ.

16.7. [redacted]

b1
b7E

(S) [redacted]

16.8. Setting Leads

(U//FOUO) Any leads concerning a CHS to be set to substantive units other than the [redacted] must be sent using a substantive case file number and [redacted] If there is no substantive case file number or if the communication contains information which identifies the CHS, in those limited instances, the [redacted] Leads for payment requests should be sent to specific personnel within the budget section of the substantive unit. These payment requests may use the CHS's file number, and the budget unit personnel may be granted access to the CHS's file for approval purposes.

b7E

16.9. Quarterly SSA Source Report Reviews

(U//FOUO) Only SSAs conduct QSSR reviews of all CHS files assigned to Agents under their supervision every 90 days. QSSR review responsibilities may not be delegated to non-Agent personnel. These reviews must be documented in the CHS's file by the reviewing SSA. An acting SSA (A/SSA) may conduct file reviews in the absence of an SSA. However, during the acting period, an ASAC must conduct the file reviews of the A/SSA's own CHSs.

(U//FOUO) When conducting file reviews, SSAs shall ensure required information, requests, and database checks are filed as required at opening, at 90 days from opening, annually, and any other appropriate time. SSAs shall ensure that instructions are documented and are timely, early approval and [redacted] are properly authorized, FBIHQ notifications are made as appropriate, and AUSA concurrences are provided if appropriate. Also, particular attention should be given to any CHS who is paid [redacted] or has engaged in unauthorized illegal activity. SSAs shall document financial audit information for each payment (see Section 17.7., SSA Financial Audit of Payments). SSAs shall ensure that payments are approved and commensurate with the value of the information being provided. SSAs should determine that statistical accomplishments are appropriately claimed, and that dissemination of a CHS's information or identity is appropriately documented. SSAs shall review CHS information used in support [redacted] Title IIIs, search warrants, affidavits, etc. SSAs shall ensure that approvals [redacted] appropriately documented. Documentation of approvals from FPO, DOJ/OEO, Legat, and CIA as required shall be reviewed. SSAs shall close the CHS if an application was not made to legalize immigration status within 90 days of opening. Furthermore, the SSAs shall ensure that proper [redacted] SSAs shall ensure compliance with the AGGs. b7E

16.10. [redacted]

(U//FOUO) Queries of [redacted] The fact that these queries were conducted shall be noted on the FOASR. Other [redacted] should be conducted annually if applicable to the CHS's situation. Derogatory information obtained must be documented in the CHS's file. b7E

16.11. [redacted]

(U//FOUO) Physical possession of a CHS's original file is never to be transferred to any individual outside the FBI [redacted] b7E

(U//FOUO) Should FBIHQ or a FO require another FO's original CHS file, in whole or in part, with SAC approval, [redacted] for shipping classified FBI information.

16.12. Requirements for Re-Openings

(U//FOUO) In order to re-open a CHS who has been previously closed, the FO must generate a new opening communication with all updated information normally required at opening. The [redacted] The opening communication must include all required [redacted] were being opened for the first time. The opening communication must indicate that the individual is being re-opened and include an explanation of the reason the CHS was previously closed. Other required checks must be completed within the first 90 days as required with an initial opening. b7E

(U//FOUO) Approval levels to re-open the CHS are the same as when the CHS was originally opened, unless the CHS was closed for cause (see Section 19, Closing a CHS) or if the CHS's status has changed such that additional approval is required (i.e., [redacted]

16.13. Closed Confidential Human Sources Re-Opened by Another FO

(U//FOUO) When a closed CHS from one FO is re-opened in another FO, the previous OO will furnish the new OO with copies of any documents in the file that are not available electronically. A copy of the entire file would be sent to the new OO upon request. Any information that reflects negatively upon the reliability of the CHS must be promptly furnished to the FO operating the CHS.

16.14. Undisclosed Participation (UDP)

(U//FOUO) [redacted]

- [redacted] b7E
- [redacted]

(U/FOUO) [redacted]

(U/FOUO) [redacted]

- [redacted] b1 b7E
- [redacted]
- [redacted]

(S)

- [redacted]
- [redacted]
- [redacted]

b7E

16.14.1. Levels of Approval

16.14.1.1. SAC Approval with CDC Review

(U/FOUO) [redacted]

- [redacted]
- [redacted]
- [redacted]

b7E

16.14.1.2. Substantive AD Approval with OGC Review

(U/FOUO) [redacted]

b7E

16.14.1.3. Director Approval

(U/FOUO) [redacted]

[redacted]

16.14.2 [redacted] and FBIHQ Determinations

(U/FOUO) [redacted] b7E

[redacted]

16.15. [redacted]

(U//FOUO) [redacted] may open and operate CHSs as permitted by [redacted] b7E

[redacted]

(U//FOUO) [redacted]

[redacted]

16.15.1 [redacted]

(U//FOUO) Approval levels for [redacted] are as follows: where this manual calls for SSA approval, the Unit Chief at [redacted] responsible for that [redacted] is the appropriate approving official; ASAC approval may be obtained from the Section Chief at [redacted] and SAC approvals may be obtained from the AD at [redacted] In addition:

- [redacted] b7E
- [redacted]
- [redacted]

- Where CDC consultation is required (e.g., the operation of a Privileged CHS), [redacted] shall consult with OGC, FBIHQ.
- As consistent with this Manual approval authorities may be delegated unless otherwise stated and approvals may be provided by those in an acting capacity or by any above-ranking official.

16.16. [redacted] Confidential Human Sources

(U//FOUO) [redacted]

b7E

[redacted]

17. Payments to Confidential Human Sources

(U//FOUO) The FBI may pay CHSs for services and expenses, including those for CHSs [redacted] This policy dictates the use of CHS funds. For case fund expenditures, contact the substantive unit. CHS payments shall be subject to the FBI's audit procedures. b7E

(U//FOUO) CHS payment documentation may be filed in the main file or in a [redacted] However, documents containing the [redacted] (Redacted copies may be filed in other sub-files.)

17.1. Confidential Human Sources Funding and Spending Authority

(U//FOUO) SAC's payment authority per CHS is automatically renewed [redacted] the beginning of each FY. In the event the SAC's annual payment authority [redacted] is expended, the FO may request additional payment authority [redacted] Requests must be submitted to the attention of [redacted] evaluates the request in coordination with the FBIHQ substantive unit. Such requests may [redacted] when operational considerations necessitate. In these situations, the request must set forth adequate justification for the enhanced spending authority. The communication must include: b7E

- [redacted]
- The dollar amount of the additional payment authority requested
- Supporting justification

17.2. Prohibitions

(U//FOUO) Under no circumstances shall any payments to a CHS be contingent upon the conviction or punishment of any individual.

(U//FOUO) In determining the way to classify a particular payment as a service or an expense to a CHS, the CA should not consider whether or not that classification might result in a basis for an impeachment at trial.

17.3. Services vs. Expenses

(U//FOUO) The payment request must distinguish between payments for services and expenses. Payment for services shall not be characterized or submitted as a payment for expenses and vice versa.

17.3.1. Services

(U//FOUO) Payments to CHSs shall be commensurate with the value of services rendered by gathering information or by their active involvement in FBI investigations. CHSs must be advised that such payments are considered taxable compensation by the

[13](U) These threshold amounts and approval authorities may be reviewed periodically and amended as deemed appropriate by the FBI Director.

Internal Revenue Service (IRS). Therefore, the FBI has an obligation to report such compensation payments, upon request by the IRS, for income tax purposes. All CHS payments for services should be made after the services have been rendered.

(U//FOUO) The CHS may pay his/her own personal expenses, which are not directly in support of an FBI investigation, out of funds received for services. However, such personal expenses unrelated to the CHS's cooperation with the FBI may not be used to justify service payments.

17.3.2. Expenses

(U//FOUO) The FBI's reimbursement of expenses incurred by a CHS shall be based on the actual expenses incurred, except that relocation expenses may be based on the estimate of the expenses (see Section 17.18, Relocation). A CHS expense is a reasonable cost incurred due to the CHS's support of an authorized investigative or intelligence matter and for which the FBI and/or U.S. Government primarily benefits. Examples of such expenditures include [redacted] b7E [redacted] at the FBI's request. The CA shall reasonably determine the amount of the expenses. Vendor receipts, copies, or the CHS's explanation for the absence of receipts shall be obtained.

(U//FOUO) CHS funds may be used for reasonable expenditures in support of the CHS's activities in investigations. The FO shall ensure that the amount reimbursed or paid for such expenses is reasonably justified based on the use or need related to the investigation.

(U//FOUO) Although [redacted] when it is deemed to be cost effective and operationally justifiable. FOs shall pay the funds to the CHS and the CHS shall [redacted] in the CHS's own name. The SAC and CDC must approve of such a purchase. b7E

(U//FOUO) If it is necessary for a CHS to have [redacted] of an FBI investigation [redacted] official use and in furtherance of an FBI investigation, the CHS [redacted] This rental may be reimbursed from CHS funds as an expense. If the CHS does not have funds for the rental, an advance of funds can be given to the CHS. Upon receipt of the rental receipt, the FBI may reimburse the CHS for the expense or, if an advance was paid, reconcile the advance with the draft office.

(U//FOUO) The FBI may reimburse a CHS for the basic maintenance of a vehicle (e.g., oil changes, tire replacement) to the extent reasonably proportionate to the vehicle's use in furtherance of an FBI investigation. These reimbursements must be reflected as an expense.

(U//FOUO) If a CHS incurs [redacted] as a direct result of his/her cooperation with the FBI (e.g., [redacted] the costs are reimbursable to the CHS upon receipt of the [redacted] These reimbursements would b7E

be classified as CHS expenses. Generally, treatment for any [redacted] b7E
[redacted] etc., are not reimbursable. However, if it is in the FBI's best interest in order to further an ongoing investigation, [redacted] can be paid with FBIHQ approval through both [redacted] and OGC.

(U//FOUO) [redacted] b7E

(U//FOUO) For the use of CHS funds for the expense of [redacted] case law has held that inducements to government witnesses may compromise a defendant's right to a fair trial. Therefore, FOs shall ensure that the government obtains the primary benefit and that reimbursements are not excessive.

(U//FOUO) CHS funds may be used to [redacted] for operational use. The CHS may retain the property if the value has diminished over the duration of the investigation to approximately [redacted] If the value exceeds this amount, the property should be recovered and inventoried or the CHS may keep the [redacted] and the remaining value must be considered a service payment and be documented as such. b7E

17.4. Payment Request and Approvals

(U//FOUO) If an FPO Attorney is participating in the conduct of an investigation or prosecution that is utilizing a CHS who is expected to testify, the FBI shall coordinate with the FPO Attorney, in advance if practicable, the payment of monies to the CHS. This can be done by obtaining the FPO's approval for a potential range of aggregate CHS payments which could be made for the duration of an investigation. If the payment is for services and the FPO Attorney objects, then no payment can be made until the dispute has been resolved through appropriate channels (see Section 20, Exceptions and Dispute Resolution, which requires that the outcome of the dispute resolution be documented in the CHS's main file).

(U//FOUO) An SAC or ASAC can approve CHS cumulative payments up to [redacted] per CHS per Fiscal Year (FY). To exceed [redacted] the FO must request approval from [redacted] (which coordinates with the substantive unit for final approval). b7E

(U//FOUO) Payments to CHSs are requested by [redacted]

- The substantive case title(s) and file number(s) for which the CHS provided the information
- The date the CHS file was opened and/or re-opened
- The total amount previously paid to the CHS during the current FY
- The total payment history that includes the total amount previously paid to the CHS by any FO of the FBI (aggregate total). If the CHS was re-opened, then include the total amount of payments as of the prior closing date(s).
- The total amount of this payment request. Payment requests for services and expenses may be included on the same draft request, although the amount for each must be specified (services vs. expenses). If a CHS is to be paid for [redacted] the SA must specify payment amounts (services vs. expenses) allotted for each program in the cover communication (e.g., [redacted] b7E
- A [redacted] for the requested payment
- [redacted] pertinent to the payment request

(U//FOUO) Vendor receipts for any CHS expense are to be obtained whenever feasible and must be attached as supporting documentation to the draft request. Exceptions include instances when requesting a receipt from the vendor would endanger the CHS or disclose the CHS's relationship with the FBI.

(U//FOUO) If an original vendor receipt cannot be attached to the draft request because it reflects the CHS's true name, the Agent must attach a copy of the receipt with the CHS's name redacted. The original vendor receipt with the CHS's true name shall be maintained in the CHS's main file.

(U//FOUO) If an original vendor receipt cannot be attached, a copy is sufficient. The copy must be maintained in the CHS's main file. Additional copies may be made as necessary to attach to the draft request.

(U//FOUO) If, for any reason, it is not possible to obtain either an original or a copy of a vendor receipt, the CA must submit a statement that the CHS advised him/her of the amount spent, note the date(s) and the reason(s) the original receipt could not be provided, and the reasonableness of the expense. For further guidance, contact [redacted] b7E

(U//FOUO) Original receipts must be maintained in the CHS's file. Copies of the receipts can be maintained in the draft office, if necessary. Before submitting the receipt, the CA must write the CHS's file number on the receipt. If the receipt bears the true name of the CHS, a redacted copy shall be submitted to the draft office with the original filed in the CHS's main file.

17.5. Paying a Confidential Human Source

(U//FOUO) After obtaining approvals outlined in the Payment Request and Approvals section above (17.4.), the CA, or any FBI Agent, obtains a payment check from the draft

office. The SA may cash the check or otherwise convert it to another form of payment to provide to the CHS. [redacted] In the event of extraordinary circumstances, which must be documented in the CHS's file, [redacted] The SAC must provide prior approval whenever feasible. If the SAC approval could not be obtained prior to the payment, then the SAC must be notified as soon as possible thereafter. The approval or notification must be documented in the CHS's file. Such waivers must be payment specific, rarely granted, and must be the exception rather than the rule. Also, in extenuating circumstances, the SAC may approve payments that are not [redacted] FBI Agent and another government official, and the CHS's [redacted] in the CHS's file. b7E

(U//FOUO) The CHS [redacted]

(U//FOUO) All CHSs who are required to pay U.S. taxes and who receive compensation from the FBI for their services must be advised that such compensation must be reported as income by them when filing federal income tax forms or other appropriate tax forms. (Complete details of any problems the CHS has encountered with the taxing authorities in relation to CHS payments should be promptly furnished to the substantive unit and [redacted]

(U//FOUO) The CHS's [redacted] The receipt must be maintained in the CHS's file. b7E

(U//FOUO) If it becomes necessary to [redacted]

17.6. Advance Expense Payments

(U//FOUO) The SAC may approve advance payments to a CHS for up to [redacted] payment for expenses totaling no more than [redacted] FY. In situations where a CHS incurs expenses in connection with his/her operation or in order to obtain information for the FBI, such as [redacted] the SAC may authorize payments in advance for these expenses prior to the expenses actually being incurred by the CHS. When funds are advanced in this manner, the FO must ensure that: 1) the actual expenses incurred by the CHS are supported with vendor receipts or, in rare instances where the receipts cannot be obtained, a CA statement as to the reasonableness of the expense and the reason given by the CHS for his/her inability to provide receipts; and 2) the actual expenses are reconciled with the advance of funds. After the CHS submits the vendor receipts and any unused funds, the CHS must sign a second receipt that reflects the actual amount spent and any funds returned by the CHS to the CA. b7E

17.7. SSA Financial Audit of Payments

(U//FOUO) At every QSSR review, the SSA shall ensure that the following requirements for paying a CHS have been completed:

- Receipt must be signed by the paying FBI Agent and witnessed by an additional government official. SAC approval or notification to waive the witness requirement must be filed if no witness was present.
- The receipt must be signed and dated by the CHS.
- The period covered must be indicated on the receipt.
- The receipt must classify the type of expenditure as services or expenses.
- The payment request may contain more than one program; however, the request must state the amount attributed to each program, i.e., Criminal, Cyber, Counterterrorism, or Counterintelligence.

Approval for the payment to the CHS must be documented.

17.8. [redacted]

(U//FOUO) A [redacted] may be utilized in circumstances in which a CHS is providing valuable information and services on a regular, predictable basis. [redacted] for the CHS. The amount of the payment must be based on the value of the services and information being provided by the CHS. [redacted] between the FBI [redacted] Payments may be made with the approved [redacted] attached to the draft request. Approved [redacted] justify each payment made without the need to comply with the detailed requirements in the Payment Request and Approvals section of this Manual (see Section 17.4., Payment Request and Approvals). SSAs are required to ensure that cooperation provided by the CHS warrants the payment. b7E

(U//FOUO) [redacted] are usually appropriate when a CHS's cooperation [redacted] are established. In the event the services and information provided by a CHS are so critical and valuable that the FBI requires the CHS to [redacted] the CHS's previous income can be used to justify the amount [redacted] Proof of income must be provided to support a [redacted] Payment for services as documented in the [redacted] is contingent on the CHS's performance. If the CHS fails to provide services and/or information warranting the amount of payment, the [redacted] may be discontinued at the FO's discretion. b7E

(U//FOUO) [redacted] are usually appropriate when the FBI [redacted] These [redacted] both parties and may be used whether or not the individual is a CHS.

(U//FOUO) Consultation with the CDC, [redacted] the appropriate substantive unit at FBIHQ, the FPO participating in the operation of the CHS, if applicable, and either the [redacted] or the [redacted] is recommended to determine whether a [redacted] is appropriate in a given case. FOs should consider that PSAs/Contracts may preclude the [redacted] at the conclusion of the investigation. [redacted] approved by the ASAC or above. All [redacted] must be submitted to [redacted] will coordinate approval with the appropriate substantive unit and FBIHQ's Finance Division/Procurement Section. b7E

17.9. Lump-Sum Payments

(U//FOUO) Lump-sum payments may be paid from FBIHQ's budget (coordinated through the budget unit of the appropriate substantive division) or the FO's budget (subject to the FO spending authority not to exceed [redacted] per CHS per FY). A FO may request a lump-sum payment for a CHS at the conclusion of any investigation in which the CHS has made significant contributions to FBI investigative matters and has not previously been compensated for those contributions. Such requests must be approved by the ASAC and submitted to [redacted] attention. b7E

(U//FOUO) Each funding request concerning any investigative program would be considered strictly on the merits of the case and the significance of the CHS's contributions to that investigation. The following issues must be addressed in any request for a lump sum payment:

- Title and character of the case to which the CHS contributed information
- Significance of the investigation
- Justification for lump-sum payment (must be for assistance not previously compensated)
- [redacted] attributed to the CHS's information or assistance and supporting the lump-sum payment b7E
- Whether the CHS suffered any financial loss (not previously compensated) as a result of his/her cooperation
- Total amount of services and total amount of expenses paid to the CHS
- If the CHS is to testify or has testified, state whether the assigned FPO concurs with the payment.
- Value of seized or forfeited property obtained as a result of his/her cooperation and whether the CHS has received or would be nominated for an award or nominated for a payment resulting from forfeited assets
- Whether the CHS has or will receive any payment for services or expenses from any other law enforcement agency(s) in connection with the information or services that he/she provided to the FBI

17.10. Payments to Confidential Human Sources by Other Field Offices

(U//FOUO) To ensure aggregate payments do not exceed payment authority, all payments to a CHS by another FO must be coordinated with the OO. The payment may be made by either another FO or OO. However, payment authority always remains the responsibility of the OO.

17.11. [redacted]

(U//FOUO) In limited circumstances, with written SAC approval, [redacted] b7E
[redacted] attached to the approved payment request and purchase of the [redacted] must be charged to the file number of the CHS as a payment for services. The Agent and a witness must document that the [redacted]

17.12. Rewards

(U//FOUO) CHSs may accept rewards offered as a result of their assistance. Rewards shall be commensurate with the value of the CHS's information or assistance. SAC approval is required to disclose the CHS's identity. If it is necessary for an Agent to receive the reward on behalf of the CHS in order to protect the CHS's identity, the Agent shall document the receipt of the reward and release the reward to the CHS. The Agent's release of the reward to the CHS shall be witnessed, and the CHS shall sign a receipt, as with any other payment. SAC or designee approval is necessary before participating in such receipt of rewards.

17.13. Forfeiture Awards

(U//FOUO) A CHS may receive an award from a forfeiture even if he/she has already been compensated for an action or for providing information which led to the forfeiture. However, any such award shall be offset by any previous payments for information or assistance which led to the seizure, excluding expense payments.

(U//FOUO) A CHS may receive compensation up to [redacted] b7E

(U//FOUO) If an award from a forfeiture is requested for a CHS, the FO must submit a communication to [redacted] upon receipt of the final order of forfeiture and prior to any equitable sharing [redacted] then coordinates the approval of the request with the Forfeiture and Seized Property Unit, FD and also prepares the approval communication and coordinates the necessary transfer of funding.

(U//FOUO) The communication must be submitted to [redacted] under the CHS number and request approval of a forfeiture award. The communication must include the following:

- Approval by an SAC or ASAC
- A copy of the final order of forfeiture

- If applicable, the name and opinion of the AUSA involved in the operation of the CHS regarding payment to the CHS with forfeited proceeds
- Total value of the forfeited property
- Amount of actual cash or residual proceeds
- Percentage of equitable sharing (the percentage of sharing is based on the remaining funds after all expenses have been deducted to include forfeiture awards)
- A detailed justification for the payment of an award including the information or assistance provided by the CHS which directly resulted in the seizure/forfeiture of the property
- Verification that the USMS has been notified of the FBI's intent to pay an award on the forfeited property (the forfeiture personnel in a FO are responsible for forwarding a communication to the USMS documenting the FBI's intent to pay an award based on the forfeiture and checking the award block on the sharing forms [DAG 72, Block F])
- State the total amount of services and total amount of expenses paid to the CHS for the FY in which the property was seized or forfeited
- Verification that the CHS has not been previously compensated for the information or assistance which led to the seizure/forfeiture of the property for which the award is being sought, or if prior payments have been made for such information or assistance, identify such payments

(U//FOUO) If the forfeited property is being placed into official use, the appraised value would be used to determine the award. All other property must be sold and the proceeds deposited by the USMS prior to a determination of the award amount.

17.14. [redacted]

(U) FBIHQ authority may be granted for a CHS to be compensated for services and expenses with [redacted] provided that all operational costs have been covered. Upon ASAC approval and concurrence of the FPO Attorney involved in the operation of the CHS, if applicable, FOs must submit a communication to [redacted] stating that all operational costs have been covered [redacted] the anticipated amount to be paid to the CHS, the name of the FPO Attorney and opinion, and the length of time for which the authority is being sought. CHSs may be paid [redacted] and/or from CHS funds; however [redacted] b7E

17.15. [redacted]

(U//FOUO) With the exception of funds paid for goods and services rendered in legitimate business transactions, any money or property [redacted] must be turned over to the FBI. Disposition of such funds would be coordinated between the FO and [redacted] with b7E

program authority over the substantive investigation (also see the NFIPM Section 30-14 for additional guidance).

17.16. Payments to a Closed Confidential Human Source

(U//FOUO) Generally, CHSs cannot be paid if they are in a closed status.

(U//FOUO) In the event a one-time only payment must be made to a CHS who has been closed, a request must be approved by the SAC. If more than one payment must be made to a CHS who has been closed, the CHS must be re-opened according to the requirements of Section 2, Opening a CHS, and Section 19.5., Future Contacts with a Closed CHS.

17.17. Vehicles

(U//FOUO) CHSs are prohibited [redacted] under which the FBI is obligated. The FBI may pay the reasonable cost of a vehicle [redacted] used to assist the FBI. (See Section 17.3.2., Expenses.) The FBI may reimburse CHSs for reasonable expenses related to the [redacted] On rare occasions, the FBI may pay expenses for the [redacted] The CHS must [redacted] (See Section 17.3.2., Expenses). Prior approval by the SAC (may not be delegated lower than ASAC) and CDC is required and must be documented to the CHS's file for the [redacted] The CHS [redacted] upon completion of operational use only if the value has [redacted] If the value exceeds this amount, the [redacted] and must be documented as such. Consultation with the CDC is recommended. b7E

17.18. [redacted]

(U//FOUO) If the CHS or his/her family is in danger because of the CHS's cooperation with the FBI, then the FBI should determine whether the [redacted] (see Section 7.1., Sponsoring a CHS into [redacted]

(U//FOUO) The justification for the [redacted] is the threat resulting from the CHS's cooperation with the FBI. A [redacted] b7E

as a guide for determining reasonable expenses for lodging, meals, and incidentals; however, these rates are not binding.

(U//FOUO) Payments intended for [redacted] require at least three estimates for moving household goods, if necessary. The estimates obtained must be maintained in the CHS's main file. To support the total amount of funds requested, amounts of the estimated costs may [redacted] etc. Because the relocation payment is based on an estimation of the actual costs, the CHS is not required to submit receipts for actual costs incurred. b7E

(U//FOUO) While this Manual governs the use of CHS funds, FOs may consider using case funds and should consult with the substantive units.

(U//FOUO) Liability associated with the move and the new location, as well as additional costs, is the responsibility of the CHS. [redacted] b7E

17.19. One Time Non-Confidential Human Source Payment

(U//FOUO) With SAC approval, only one payment may be made to any individual who has provided information to the FBI in furtherance of an FBI investigation, but who has never been opened as a CHS for the FBI. The limits and requirements described in this section apply to non-CHS payments. For payments in excess of [redacted] a communication requesting the amount desired with justification must be submitted to [redacted] for approval. A non-CHS may only be paid for services rendered and/or expenses of that individual as defined above in Section 17.3., Services vs. Expenses. Payments to non-CHSs are charged to the CHS budget using the substantive case file number. b7E

(U//FOUO) Before approving a payment to a non-CHS, the SAC should weigh the [redacted] b7E

(U//FOUO) Non-CHS payments may not be used for reimbursing expenses of Agents or other law enforcement/intelligence community officials.

(U//FOUO) The FO HSC must open a file dedicated to tracking payments to non-CHSs in order to capture that person's information and to help prevent more than one payment being made to a non-CHS.

17.20. Payments to Individuals Who Are Not FBI Confidential Human Sources for [redacted]

(U//FOUO) CHS funds may not be used for [redacted] of individuals who have never been opened as an FBI CHS but who require [redacted] because of their cooperation with the FBI or [redacted] Draft requests, payment requests, the [redacted] etc. should not use the term CHS or "non-CHS" when referring to these individuals. Payments to these individuals must be made from the budget of the FO or substantive investigative program. b7E

18. Requirements When a Confidential Human Source is Injured or Killed

(U//FOUO) When a CHS is seriously injured or killed as a result of his/her cooperation with the FBI, the FO operating the CHS must immediately notify [redacted] and the substantive unit. A communication explaining the details surrounding the incident must be forwarded to both the [redacted] and the substantive unit as soon as possible. b7E

(U//FOUO) When a CHS is killed as a result of his/her cooperation with the FBI [redacted]

[redacted]

19. Closing a Confidential Human Source

19.1. Closing Communication

(U) The list of reasons for closing CHSs is a guide but does not mandate the closing of a CHS under any particular circumstance. When a determination has been made to close a CHS for any reason (see Section 19.2., Coordination with the FPO), a communication documenting the reason for closing must be included in the CHS's main file.

(U) General Reasons for Closing are:

- Confidentiality unintentionally revealed
- Cooperation completed
- Death
- Approval to operate was denied by FBIHQ
- [redacted] b7E
- Poor health
- Requested termination
- Transfer of Agent
- Relocated/Unavailable
- Unproductive
- CHS no longer in a position to report

[redacted] b7E

- [redacted]

(U) Upon closing, the CA or Co-CA and one other government official (one person present must be an FBI Agent) [redacted] that b7E

[redacted]

witnessed by at least one FBI Agent, and one other government official. SSAs must review all closing documentation. Furthermore, if the [redacted] b7E
[redacted] (See Section 10.9., Revocation of Authorization.)

19.2. Coordination with the FPO

(U) If an FPO Attorney had participated in the conduct of an investigation utilizing a CHS, the CA or Co-CA shall coordinate with the FPO attorney, in advance, whenever possible, regarding any decision to close a CHS.

19.3. Delayed Notification

(U) In the event the CA or Co-CA has determined that there is sufficient reason to close a CHS and that providing an [redacted] b7E
[redacted] That decision and the reasons supporting it must be documented in the CHS's file.

(U) If an FPO Attorney had participated in the conduct of an investigation utilizing a CHS, the CA or Co-CA shall coordinate with the FPO attorney, in advance, whenever possible, regarding any decision to delay notification of closing to the CHS.

19.4. Future Contacts with Closed Confidential Human Sources

(U) Absent exceptional circumstances that are approved by an SSA, in advance whenever possible, an FBI Agent [redacted] Such approval must be documented in the CHS's main file. Further, if approved, such contact must be coordinated, in advance whenever possible, with an FPO, if any, who is participating in the conduct of an investigation which utilizes that CHS or if the CHS is expected to testify. b7E

(U) CHSs who were closed, [redacted] may be re-contacted without prior approval. New information may be documented to a closed CHS file; however, the CHS should be reopened if the relationship between the FBI and the CHS would be ongoing.

(U) To make payments to a closed CHS, see Section 17.16., Payments to a Closed CHS.

20. Exceptions and Dispute Resolution

(U//FOUO) As provided by the AGGs CHS, whenever an FBI AD, ADIC, SAC, CFP, or their respective designee(s) believes that extraordinary circumstances exist that warrant an exception to any provision of the AGGs CHS, or whenever there is a dispute between or among entities regarding the AGGs, an exception must be sought from, or the dispute shall be resolved by, the DOJ's AAG for the Criminal Division or the NSD, whichever is appropriate, or his/her designee. Disagreements thereafter shall be resolved by DOJ's DAG, AG, or designee.

(U//FOUO) Whenever there is a dispute with the AAG for either the Criminal Division or NSD of the DOJ, such dispute shall be resolved by the DAG or his/her designee.

(U//FOUO) Any exception granted or dispute resolved pursuant to Section 20, Exceptions and Dispute Resolution, shall be documented in the CHS's main file.

Appendix A: [redacted]

(U//FOUO) The DOJ and FBI are currently revising all [redacted] When these new AGGs CHS become available, they will be contained herein as Appendix A.

(S) [redacted]

b1
b7E

(U//FOUO) The administrative requirement to obtain [redacted] as [redacted] All other authorizations, coordination, and approvals must still be obtained from the appropriate substantive division, Legat, Chief of Mission and/or DOJ Office of International Affairs as appropriate. Procedures for those requests remain the same.

(S) # Appendix B: [redacted]

[redacted]

b1

(S) [redacted]

Appendix C: Legal Authorities

(U//FOUO) The new Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources, signed on December 13, 2006, eliminated various types of cooperating witnesses, confidential informants, and assets covered under FBI policy.

(U//FOUO) Under the authority of the new Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources, this Confidential Human Source Policy Manual was required in order to implement and comply with mandates to comprehensively address all CHS administration.

Appendix D: Sources of Additional Information

Please view the Directorate of Intelligence's web site for additional information:

[redacted]

b6
b7C
b7E

Directorate of Intelligence

[redacted] Unit Chief, [redacted]

Appendix E: Key Words and Acronyms

Key Words

Confidential Human Source: Any individual who is believed to be providing useful and credible information to the FBI for any authorized information collection activity, and from whom the FBI expects or intends to obtain additional, useful, and credible information in the future, and whose identity, information, or relationship with the FBI warrants confidential handling.

Acronyms

AAG	Assistant Attorney General
AD	Assistant Director
ADIC	Assistant Director in Charge
ALAT	Assistant Legat Attaches
AGG	Attorney General's Guidelines
AGG CHS	Attorney General's Guidelines Regarding the Use of FBI Confidential Human Sources
ASAC	Assistant Special Agent in Charge
A/SSA	Acting Supervisory Special Agent
AUSA	Assistant United States Attorney
BOP	Bureau of Prisons
CA	Case Agent
CDC	Chief Division Counsel
CE	Confidential Expenditures
[redacted]	
CFP	Chief Federal Prosecutor
CHS	Confidential Human Source
CHSC	Confidential Human Source Coordinator
CHSPM	Confidential Human Source Policy Manual
CHSVSM	Confidential Human Source Validation Standards Manual
[redacted]	
CIP	Criminal Informant Program

b7E

CIS	Citizenship and Immigration Services
[redacted]	
DAD	Deputy Assistant Director
DAG	Deputy Attorney General
DEA	Drug Enforcement Administration
DD	Deputy Director
DHS	Department of Homeland Security
DI	Directorate of Intelligence
DO	Doctor of Osteopathy
DoD	Department of Defense
DOE	Department of Energy
DOJ	Department of Justice
DOS	Department of State
EC	Electronic Communication
ECPA	Electronic Communications Privacy Act
ELSUR	Electronic Surveillance
FBI	Federal Bureau of Investigation
FBIHQ	Federal Bureau of Investigation Headquarters
FD	Finance Division
[redacted]	
FO	Field Office
FOASR	Field Office Annual Source Report
FPO	Federal Prosecuting Office
FY	Fiscal Year
[redacted]	
HSRC	Human Source Review Committee
HUMINT	Human Intelligence

b7E

b7E

ICE	Immigration and Customs Enforcement
IIR	Intelligence Information Report
[redacted]	
INR	Bureau of Intelligence and Research
INS	Immigration and Naturalization Service
IRS	Internal Revenue Service
LHM	Letterhead Memorandum
MAOP	Manual of Administrative Operations and Procedures
MD	Doctor of Medicine
MIOG	Manual of Investigative Operations and Guidelines
MOU	Memorandum of Understanding
[redacted]	
NCIC	National Crime Information Center
NFIPM	National Foreign Intelligence Policy Manual
NFPO	No Foreign Policy Objection
NSD	National Security Division
NSIG	National Security Investigation Guidelines
NSLB	National Security Law Branch
OCA	Office of Congressional Affairs
OCDETF	Organized Crime Drug Enforcement Task Force
ODNI	Office of the Director of National Intelligence
OEO	Office of Enforcement Operations
OGC	Office of General Counsel
OIO	Office of International Operations
OO	Office of Origin
[redacted]	
SA	Special Agent
SAC	Special Agent in Charge
[redacted]	

b7E

b7E

b7E

SSA	Supervisory Special Agent
SSN	Social Security Number
[redacted]	
TFO	Task Force Officer
UCC	Undercover Coordinator
UCE	Undercover Employee
UCO	Undercover Operation
UN	United Nations
UNI	Universal Index
USA	United States Attorney
USAM	United States Attorney Manual
US	United States
USPC	United States Parole Commission
USAO	United States Attorney's Office
USMS	United States Marshal Service

b7E

b7E

[redacted]

FEDERAL BUREAU OF INVESTIGATION
FOIPA
DELETED PAGE INFORMATION SHEET

No Duplication Fees are charged for Deleted Page Information Sheet(s).

Total Deleted Page(s) ~ 6
Page 42 ~ b1
Page 43 ~ b7E
Page 44 ~ b7E
Page 45 ~ b7E
Page 46 ~ b7E
Page 64 ~ b7E

NFIPM Section 28 (U) Undercover Operations

Section 28-01 (U) Undercover Operations

A. (U) The Attorney General Guidelines for National Security Investigations (NSIG) permit the FBI to conduct undercover operations during the course of preliminary or full investigations. The NSIG, however, do not provide guidance as to how such undercover operations should be conducted. While there are Attorney General Guidelines which pertain to undercover operations in support of FBI criminal investigations, they are not controlling with respect to FBI NFIP undercover operations. Field Offices should contact the Undercover Program Managers of the Counterintelligence Division or Counterterrorism Division (as appropriate) for current policy and procedure regarding National Security Undercover Operations.

B. (U) Undercover operations involve FBI employees who engage in relationships with investigative targets over extended periods of time, while concealing their employment with the FBI. If there have been [redacted] and the emphasis shifts from target of opportunity to priority target, and the field office wishes to continue these contacts, a Group I undercover proposal must be approved by FBI Headquarters or a Group II proposal by the SAC. b7D b7E

1. Employees in Undercover operations are administered [redacted] They are not, however, subject to periodic evaluations.

2. Undercover operations require Case Agents as well as undercover employees. Undercover employees should generally not serve in the case agent capacity, in order that impartial perspectives on targets and operations may be provided.

C. (U) The following activities are not undercover operations: lookouts; physical surveillances; double agents; pretext interviews; [redacted] and contacts with targets of opportunity, using [redacted] when continued contact is not anticipated. b7E

(U) D. (U) Undercover operations may only be employed within the context of appropriately authorized [redacted]

(S) [redacted] b1

F. (U) Undercover operations which do not progress towards their declared objectives within suitable periods of time should be redirected at alternate targets, or terminated.

G. (U) Undercover operations are categorized as either Group I or Group II.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret

Section 28-02 (U) Group I

A. (U) Group I operations involve sensitive circumstances

1. Sensitive circumstances are invoked when the following types of persons and organizations are the targets of undercover operations:

2. Sensitive circumstances are also invoked when undercover employees engage in the following types of activities

b7E

3. Finally, sensitive circumstances are invoked whenever FBI undercover operations involve

(S)

b1

b7E

(U) E. (X) authorizations for Group I Undercover operations may be authorized for

b7E

1. Requests for extensions must be submitted six weeks prior to expiration dates; set forth the current initiation and termination dates; and again address all the factors which are set forth above to also include: accomplishments thus far, new objectives, expenditures and requested budget and any stipulations previously applied to the Group I.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Secret

Section 28-03 (U) Group II

b7E

A. (U) Group II Undercover operations are authorized

C. (U) As is the case with Group I undercover operations, authorizations for Group II undercover operations are for b7E

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 28-04 (U) Undercover Administrative Matters

A. (U) All undercover operations must be assigned codewords, and they must be utilized in all communications concerning them (including initial proposals). The captions of initial undercover operation proposals should adhere to the following format:
"Codeword"
FCI- or IT-
Undercover Proposal
B. (U) Undercover employee are established merely for administrative purposes, in order to support employee activities. Therefore, expenditures in connection with undercover operations do not derive from funding. Rather, expenditures associated with NFIP undercover operations must be charged to using their substantive case file numbers. See: Confidential Funding Guide, Section 8.3.6. b7D b7E
1. However, payments in connection with undercover operations, or who work exclusively in support of undercover operations must be made from funds, rather than funds.
2. Field supervisors are responsible for the accountability of funds used in undercover operations. See: Confidential Funding Guide, generally.
C. (U) All undercover operations require periodic submissions

D. (U) With respect to otherwise illegal activities which, in connection with undercover operations, may be engaged in, see, generally: Section 2-24, supra. b7E

must be approved, in advance, by the SAC.
appropriate officials of those agencies must be advised of this fact, unless the undercover operation would be

jeopardized by doing so [redacted] must be made at the FBI Headquarters level.

[redacted] the National Security Undercover Review Committee must review and approve the matter before any other authorizations are sought.

3. [redacted] b7E However, every effort should be made to discuss the matter with an SAC beforehand, and to suitably advise FBI Headquarters.

[redacted] In such events, reports concerning the activities engaged in must be made to the SAC, and the SAC must submit full reports to FBI Headquarters.

b) The foregoing notwithstanding, [redacted] under such b7E circumstances must be reported to FBI Headquarters as soon as possible after the events.

4. [redacted] this must also be reported to FBI Headquarters as soon as possible after the fact.

5. As set forth in the 1988 Attorney General Procedure For Reporting And Use of Information Concerning Violations Of Law And Authorization For Participation In Otherwise Illegal Activities In FBI Foreign Intelligence, Counterintelligence Or International Terrorism Intelligence Investigations, authorization to engage in otherwise illegal activity must be approved in advance by the SAC and, in most cases by the appropriate Department of Justice official. The National Security Law Branch should be consulted prior to seeking authorization for otherwise illegal activity.

E. (U) Both the CD and CTD Undercover Coordinators maintain a list of personnel who have indicated an interest in participating in undercover activities; and the identities of all personnel who are being considered for undercover assignments, along with their qualifications, must be supplied to FBI Headquarters. Potential candidates for undercover assignments should be evaluated on the basis of the following criteria: [redacted] b7E

G. (U) Certain activities within the contexts of undercover operations may also require additional authorization; e.g.,

1. UDP. See Section 27-27, supra.
2. Director and Attorney General authorization to deposit appropriated funds or earned income into financial institutions; use appropriated funds to lease space; establish a proprietary; and use earned income to offset operational expenses.

EFFDATE: 04/29/2002 MCRT# 1262 Div. D5 Cav: SecClass: Unclassified

Section 30 (U) Double Agents and Double Agent Operations

Superseded by Corporate Policy Directive #0309D, titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010.

Section 30-5 superseded by Corporate Policy Directive #0309D , titled "Counterintelligence Division Policy Implementation Guide", dated 08/09/2010, and the Confidential Human Sources Manaual (CHSM), dated 09/05/2007.

Eff. Date: 08/09/2010